目　　录

第五章　剩余系，欧拉定理、费尔马定理及其应用

§1. 应用方面的例子

设 a，b，c，d 都是正整数．令 $a^0=1$，$a^1=a$，$a^2=a\times a$，$a^3=a\times a\times a$．当 n 是一个大于 1 的正整数时，我们用 a^n 来表示由 n 个相同的 a 相乘所得的积．我们还用 a^{b^n} 来表示由 b^n 个相同的 a 相乘所得的积．由于 $3^4=3\times3\times3\times3=81$，所以有

$$2^{3^4}=2^{81}>10^{24}>10^4>(2^3)^4.$$

由于 $4^5=1024$，所以有

$$3^{4^5}=3^{1024}>10^{488}>(81)^5=(3^4)^5.$$

因而

$$2^{3^4}>10^{20}\times(2^3)^4,\quad 3^{4^5}>10^{478}\times(3^4)^5.$$

由于 $5^6=15625$，$6^7=279936$，所以有

$$4^{5^6}=4^{15625}>10^{9407},\quad 5^{6^7}=5^{279936}>10^{195666}.$$

但是

$$(4^5)^6=(1024)^6<10^{19},\quad (5^6)^7=(15625)^7<10^{30},$$

因而

$$4^{5^6}>10^{9388}\times(4^5)^6,\quad 5^{6^7}>10^{195636}\times(5^6)^7.$$

我们用 $a^{b^{c^n}}$ 来表示由 b^{c^n} 个相同的 a 相乘所得的积，所以有

$$3^{4^{5^6}}=3^{4^{15625}}\geqslant 10^{10^{9406}},\quad 4^{5^{6^7}}>10^{10^{195665}},$$

$$(3^{4^5})^6=\quad 3^{1024\times6}=3^{6144}\leqslant 10^{2932},$$

$$(4^{5^6})^7=4^{15625\times7}=\ 4^{109375}\leqslant 10^{65851}.$$

我们又有

$$(12345^{56}+50)^{40} \leqslant (10^{230})^{40} = 10^{9200} \leqslant 10^{9407} \leqslant 4^{5^6}.$$

设A是一个小于 7 的非负整数. 在本章中将证明，如果今天是星期天，从今天起再经过 a^{b^c} 天后是星期 A，那么从今天起再经过 $a^{b^{c^n}}$ 天后，也是星期A. 其中 n 是任意正整数，而星期 0 定义为星期天. 如果今天是星期天，那么使用本章中所讨论的方法，容易计算出从今天起再经过 a^{b^c} 天后是星期几。

例 1 如果今天是星期一，c 是一个正整数，那么从今天起再过 773^{3169^c} 天后，应该是星期四.

在本章 §5 中将对例 1 加以证明. 令m是一个正整数，使用本章中所讨论的方法可以计算出 $(a^b+c)^d$ 被m除的余数。

例 2 求证 $(12371^{56}+34)^{28+72c}$ 被 111 除的余数等于 70，其中 c 是任意非负整数.

在本章 §5 中将给出例 2 的证明. 我们将在第六章说明欧拉定理、费尔马定理在研究循环小数时的作用.

§2. 完全剩余系

设 a, b 是任意二个整数，m是一个正整数，如果存在一个整数q，使得 $a-b=mq$ 成立，我们就说 a, b 对模m同余，记作 $a \equiv b \pmod m$.

引理 1 如果 a, b, c 是任意三个整数，m是一个正整数，则当 $a\equiv b \pmod m$, $b \equiv c \pmod m$ 成立时，有

$$a \equiv c \pmod m.$$

证 由 $a-b=mq_1$, $b-c=mq_2$, 其中 q_1, q_2 是二个整数，得到 $a-b+b-c=mq_1+mq_2$. 故有 $a-c=m(q_1+q_2)$, 其中 q_1+q_2 是一个整数.

引理 2 如果 a, b, c 是任意三个整数，m 是一个正整数且 $(m, c)=1$，则当 $ac \equiv bc \pmod{m}$ 时，有

$$a \equiv b \pmod{m}.$$

证 由于 $c(a-b)=ac-bc=mq$，其中 q 是一个整数，$(m, c)=1$，我们有 $a-b=mq_1$，其中 q_1 是一个整数.

引理 3 如果 a, b 是任意二个整数，而 m, n 是二个正整数，则当 $a \equiv b \pmod{m}$ 时，有

$$a^n \equiv b^n \pmod{m}.$$

证 由 $a-b=mq$，其中 q 是一个整数，我们有

$$a^n=(b+mq)^n=b^n+\cdots+(mq)^n=b^n+mq_1,$$

其中 q_1 是一个整数. 故有 $a^n-b^n=mq_1$，即

$$a^n \equiv b^n \pmod{m}.$$

我们把 0，1 叫作模 2 的不为负最小完全剩余系. 我们把所有偶整数(即 $2n$ 形状的所有整数，其中 $n=0, \pm 1, \pm 2, \cdots$)划成一类，把所有奇整数(即 $2n+1$ 形状的所有整数，其中 $n=0, \pm 1, \pm 2, \cdots$)划成一类. 这样我们就把全体整数分成为 2 类，即偶整数类和奇整数类. 从偶整数类中任意取出一个整数 a_1，从奇整数类中任意取出一个整数 a_2. 我们把 a_1，a_2 叫作模 2 的一个完全剩余系. 例如 0，3 是模 2 的一个完全剩余系，而 1，6 也是模 2 的一个完全剩余系. 如果 a_3 是一个奇整数而 a_4 是一个偶整数(或 a_3 是一个偶整数而 a_4 是一个奇整数)，则 a_3，a_4 是模 2 的一个完全剩余系. 所以说模 2 的完全剩余系的个数有无限多个.

设 m 是一个大于 2 的整数，我们把 $0, 1, \cdots, m-1$ 叫作模 m 的不为负最小的完全剩余系. 我们把能被 m 整除的所有整数(即 mn 形状的所有整数，其中 $n=0, \pm 1, \pm 2, \cdots$)划成一类；把被 m 除后，余数是 1 的所有整数(即 $mn+1$ 形状的所有整数，其中 $n=0, \pm 1, \pm 2, \cdots$) 划成一类；…；把被 m

除后，余数是 $m-1$ 的所有整数(即 $mn+m-1$ 形状的所有整数，其中 $n=0, \pm1, \pm2, \cdots$) 划成一类；这样我们就把全体整数分成为 m 类. 如果从每一类当中各取出一个整数，则这 m 个整数就叫作模 m 的一个完全剩余系.

例 3 求证 $-10, -6, -1, 2, 10, 12, 14$ 是模 7 的一个完全剩余系.

证 由于

$-10\equiv 4 \pmod 7$, $-6\equiv 1 \pmod 7$, $-1\equiv 6 \pmod 7$, $2\equiv 2 \pmod 7$, $10\equiv 3 \pmod 7$, $12\equiv 5 \pmod 7$, $14\equiv 0 \pmod 7$,

而 $4, 1, 6, 2, 3, 5, 0$ 和 $0, 1, 2, 3, 4, 5, 6$ 只是在次序上有不同，故 $-10, -6, -1, 2, 10, 12, 14$ 是模 7 的一个完全剩余系.

例 4 求证 $6, 9, 12, 15, 18, 21, 24, 27$ 是模 8 的一个完全剩余系.

证 由于

$$6\equiv 6 \pmod 8,\quad 9\equiv 1 \pmod 8,\quad 12\equiv 4 \pmod 8,$$
$$15\equiv 7 \pmod 8,\quad 18\equiv 2 \pmod 8,\quad 21\equiv 5 \pmod 8,$$
$$24\equiv 0 \pmod 8,\quad 27\equiv 3 \pmod 8,$$

而 $6, 1, 4, 7, 2, 5, 0, 3$ 和 $0, 1, 2, 3, 4, 5, 6, 7$ 只是在次序上有不同，故 $6, 9, 12, 15, 18, 21, 24, 27$ 是模 8 的一个完全剩余系.

引理 4 设 m 是一个大于 1 的整数，$a_1, a_2, \cdots, a_m$ 是模 m 的一个完全剩余系. 如在 $a_1, a_2, \cdots, a_m$ 中任取出二个整数，则这二个整数对模 m 是不同余的.

证 以 m 为模，则任何一个整数一定和下列 m 个整数

$$0, 1, \cdots, m-1$$

之一同余. 令 r_i (其中 $i=1, 2, \cdots, m$) 是一个整数，满足条

件

$$a_i \equiv r_i (\bmod m), \quad 0 \leqslant r_i \leqslant m-1, \tag{1}$$

则我们有

$$a_1 \equiv r_1 (\bmod m),\ a_2 \equiv r_2 (\bmod m), \cdots, a_m \equiv r_m (\bmod m). \tag{2}$$

其中 $0 \leqslant r_1 \leqslant m-1, 0 \leqslant r_2 \leqslant m-1, \cdots, 0 \leqslant r_m \leqslant m-1$. 由于 $a_1, a_2, \cdots, a_m$ 是模 m 的一个完全剩余系，所以 $r_1, r_2, \cdots, r_m$ 和 $0, 1 \cdots, m-1$ 只是在次序上可能有不同. 由于在 $0, 1, \cdots, m-1$ 中，任取出二个整数，这二个整数对模 m 是不同余的，所以在 $r_1, r_2, \cdots, r_m$ 中任取出二个整数，这二个整数对模 m 是不同余的. 故由(2)式知道，在 $a_1, a_2, \cdots, a_m$ 中任取出二个整数，则这二个整数对模 m 是不同余的.

引理 5 设 m 是一个大于 1 的整数，而 $a_1, a_2, \cdots, a_m$ 是 m 个整数，又设在 $a_1, a_2, \cdots, a_m$ 中任取出二个整数时，这二个整数对模 m 是不同余的，则 $a_1, a_2, \cdots, a_m$ 是模 m 的一个完全剩余系.

证 以 m 为模，则任何一个整数一定和下列 m 个整数

$$0, 1, \cdots, m-1$$

之一同余. 令 r_i（其中 $i=1, 2, \cdots, m$）是一个整数，满足条件

$$a_i \equiv r_i (\bmod m), \quad 0 \leqslant r_i \leqslant m-1,$$

则我们有

$$a_1 \equiv r_1 (\bmod m),\ a_2 \equiv r_2 (\bmod m), \cdots, a_m \equiv r_m (\bmod m). \tag{3}$$

其中 $0 \leqslant r_1 \leqslant m-1,\ 0 \leqslant r_2 \leqslant m-1, \cdots, 0 \leqslant r_m \leqslant m-1$. 由于(3)式和假设在 $a_1, a_2, \cdots, a_m$ 中任取出二个整数时，这二个整数对模 m 不同余，所以当我们在 $r_1, r_2, \cdots, r_m$ 中任取出二个整数时，这二个整数对模 m 不同余. 所以 $r_1, r_2, \cdots, r_m$ 和 $0, 1, \cdots, m-1$ 只是在次序上可能有不同，即 $a_1, a_2, \cdots, a_m$ 是模 m 的一个完全剩余系.

引理 6 设m是一个大于 1 的整数，而 $a_1, a_2, \cdots, a_m$ 是模m的一个完全剩余系，则当 b 是一个整数时，$a_1+b, a_2+b, \cdots, a_m+b$ 也是模m的一个完全剩余系。

证 设在 $a_1+b, a_2+b, \cdots, a_m+b$ 中存在二个整数 $a_k+b, a_\lambda+b$（其中 $1 \leqslant k < \lambda \leqslant m$），使得

$$a_k+b \equiv a_\lambda+b \pmod m \tag{4}$$

成立．我们又有

$$b \equiv b \pmod m. \tag{5}$$

由 (4) 式减去 (5) 式，得到

$$a_k \equiv a_\lambda \pmod m. \tag{6}$$

由引理 4 和 $a_1, a_2, \cdots, a_m$ 是模m的一个完全剩余系，知道 (4) 式是不可能成立的．所以在 $a_1+b, a_2+b, \cdots, a_m+b$ 中任取出二个整数时，这二个整数对模m不同余，而由引理 5 知道 $a_1+b, a_2+b, \cdots, a_m+b$ 是模m的一个完全剩余系．

引理 7 设m是一个大于 1 的整数，b 是一个整数且满足条件 $(b, m)=1$．如果 $a_1, a_2, \cdots, a_m$ 是模m的一个完全剩余系，则 $ba_1, ba_2, \cdots, ba_m$ 也是模m的一个完全剩余系．

证 设在 $ba_1, ba_2, \cdots, ba_m$ 中存在二个整数 ba_k, ba_λ（其中 $1 \leqslant k < \lambda \leqslant m$），使得

$$ba_k \equiv ba_\lambda \pmod m \tag{7}$$

成立，则由 $(b, m)=1$ 和引理 2 我们有

$$a_k \equiv a_\lambda \pmod m. \tag{8}$$

由引理 4 和 $a_1, a_2, \cdots, a_m$ 是模m的一个完全剩余系，知道(7) 式是不可能成立的．所以在 $ba_1, ba_2, \cdots, ba_m$ 中任取出二个整数时，这二个整数对模m不同余，而由引理 5 知道 $ba_1, ba_2, \cdots, ba_m$ 是模m的一个完全剩余系．

引理 8 设m是一个大于 1 的整数，而 b, c 是二个任意的整数但满足条件 $(b, m)=1$．如果 $a_1, a_2, \cdots, a_m$ 是模m

的一个完全剩余系，则 $ba_1+c, ba_2+c, \cdots, ba_m+c$ 也是模 m 的一个完全剩余系.

证 由于 $a_1, a_2, \cdots, a_m$ 是模 m 的一个完全剩余系，从引理 7 和 $(b, m)=1$ 知道 $ba_1, ba_2, \cdots, ba_m$ 也是模 m 的一个完全剩余系. 由于 $ba_1, ba_2, \cdots, ba_m$ 是模 m 的一个完全剩余系，从引理 6 和 c 是一个整数知道 $ba_1+c, ba_2+c, \cdots, ba_m+c$ 也是模 m 的一个完全剩余系.

例 5 使用引理 8 来证明例 4 中的结果.

证 在引理 8 中取 $m=8, b=3, c=6, a_i=i-1$ (其中 $1\leqslant i\leqslant 8$). 由于 0, 1, 2, 3, 4, 5, 6, 7 是模 8 的一个完全剩余系，并且 $ba_1+c=6$, $ba_2+c=9$, $ba_3+c=12$, $ba_4+c=15$, $ba_5+c=18$, $ba_6+c=21$, $ba_7+c=24$, $ba_8+c=27$, 故由引理 8 知道 6, 9, 12, 15, 18, 21, 24, 27 是模 8 的一个完全剩余系.

引理 9 如果 m 是一个大于 1 的整数而 a, b 是任意的二个整数，使得

$$a\equiv b \pmod m$$

成立，则有 $(a, m)=(b, m)$.

证 由 $a\equiv b \pmod m$ 得到 $a=b+mt$, 其中 t 是一个整数，故有 $(b, m)\mid a$. 又由 $(b, m)\mid m$ 得到 $(b, m)\mid(a, m)$. 由 $b=a-mt$ 有 $(a, m)\mid b$. 又由 $(a, m)\mid m$ 得到 $(a, m)\mid(b, m)$. 故由 $(b, m)\mid(a, m)$ 和 $(a, m)\mid(b, m)$ 得到 $(a, m)=(b, m)$.

§ 3. 欧拉函数 $\varphi(m)$

定义 1 我们用 $\varphi(m)$ 来表示不大于 m 而和 m 互素的正整数的个数. 我们把 $\varphi(m)$ 叫做欧拉 (Euler) 函数.

因为无论 n 是什么整数，我们都有 $(n, 1)=1$, 所以 1 和任何正整数都是互素的. 我们又有 $\varphi(1)=1$.

引理 10 设 l 是一个正整数，p 是一个素数，则我们有

$$\varphi(p^l)=p^{l-1}(p-1).$$

证 由于 1，2，…，$p-1$ 中的任何一个整数都是和 p 互素的，故有 $\varphi(p)=p-1$. 当 $l=1$ 时有 $p^{l-1}=p^0=1$，因而当 $l=1$ 时本引理成立．现设 $l>1$，不大于 4 而和 4 互素的正整数是 1，3，共有 2 个，故有 $\varphi(4)=2$. 不大于 8 而和 8 互素的正整数是 1，3，5，7，共有 4 个，故有 $\varphi(8)=4$. 不大于 9 而和 9 互素的正整数是 1，2，4，5，7，8 共有 6 个，故有 $\varphi(9)=6$. 而满足条件 $l>1$ 及 $p^l\leqslant 9$ 的 p^l 只有 4，8，9 这三个数，并且 $\varphi(2^2)=\varphi(4)=2=2^{2-1}(2-1)$，$\varphi(2^3)=\varphi(8)=4=2^{3-1}(2-1)$，$\varphi(3^2)=\varphi(9)=6=3^{2-1}(3-1)$，故当 $l>1$ 而 $p^l\leqslant 9$ 时本引理成立．现设 $l>1$ 而 $p^l\geqslant 10$. 在不大于 p^l 的正整数中(共有 p^{l-1} 个整数，即)

$$p,2p,3p,\cdots,p^{l-1}p$$

是 p 的倍数，而其余的不大于 p^l 的正整数都是和 p 互素的．又不大于 p^l 的正整数共有 p^l 个，而其中是 p 的倍数的正整数有 p^{l-1} 个，故不大于 p^l 而和 p^l 互素的正整数的个数是 p^l-p^{l-1}，即

$$\varphi(p^l)=p^l-p^{l-1}=p^{l-1}(p-1).$$

由引理 10 得到 $\varphi(2)=1$，$\varphi(3)=2$，$\varphi(4)=2$，$\varphi(5)=4$，$\varphi(7)=6$，$\varphi(8)=4$，$\varphi(9)=6$，$\varphi(11)=10$，$\varphi(13)=12$，$\varphi(16)=8$，$\varphi(17)=16$，$\varphi(19)=18$.

§4. 简化剩余系

如果 m 是一个大于 1 的整数，由定义 1 知道不大于 m 而和 m 互素的正整数有 $\varphi(m)$ 个．现设 $1<a_2<\cdots<a_{\varphi(m)}$ 是不大于 m 而和 m 互素的全体正整数．我们把被 m 除后，余数是 1 的所有整数(即 $mn+1$ 形状的所有整数，其中 $n=0$，

$\pm 1, \pm 2, \cdots$)划成一类. 把被m除后,余数是a_2的所有整数(即$mn + a_2$形状的所有整数,其中$n = 0, \pm 1, \pm 2, \cdots$)划成一类,…,把被$m$除后, 余数是$a_{\varphi(m)}$的所有整数(即$mn + a_{\varphi(m)}$形状的所有整数,其中$n = 0, \pm 1, \pm 2, \cdots$)划成一类. 以$m$为模,则任何一个整数一定和下列$m$个整数

$$0, 1, \cdots, m-1$$

之一同余. 由引理9知道, 如果a和b对于模m同余, 则由$(a, m) = 1$可得到$(b, m) = 1$. 因而以m为模,任何一个和m互素的整数一定和下列$\varphi(m)$个整数

$$1, a_2, \cdots, a_{\varphi(m)}$$

之一同余. 故按照前面分类的方法,我们就把全体和m互素的整数分成为$\varphi(m)$类. 从每一类当中各取出一个整数,则这$\varphi(m)$个整数就叫做以m为模的一个简化剩余系.

例6 求证4, 8, 16, 28, 32, 44, 52, 56是模15的一个简化剩余系.

证 由于小于15而和15互素的正整数共有8个,即

$$1, 2, 4, 7, 8, 11, 13, 14,$$

我们有

$$4 \equiv 4 \pmod{15}, \quad 8 \equiv 8 \pmod{15}, \quad 16 \equiv 1 \pmod{15},$$
$$28 \equiv 13 \pmod{15}, \quad 32 \equiv 2 \pmod{15}, \quad 44 \equiv 14 \pmod{15},$$
$$52 \equiv 7 \pmod{15}, \quad 56 \equiv 11 \pmod{15}.$$

由于4, 8, 1, 13, 2, 14, 7, 11和1, 2, 4, 7, 8, 11, 13, 14只是在次序上不同,所以4, 8, 16, 28, 32, 44, 52, 56是模15的一个简化剩余系.

引理11 设m是一个大于1的整数$b_1, b_2, \cdots, b_{\varphi(m)}$是模$m$的一个简化剩余系. 如在$b_1, b_2, \cdots, b_{\varphi(m)}$中任取出二个整数,则这二个整数对模$m$是不同余的. 如在$b_1, b_2, \cdots, b_{\varphi(m)}$中任取出一个整数,则这个整数是和$m$互素的.

证 设$1<a_2<\cdots<a_{\varphi(m)}$是不大于$m$而和$m$互素的全体正整数. 令$r_i$(其中$i=1,2,\cdots,m$)是一个整数,满足条件

$$b_i\equiv r_i(\mathrm{mod}\, m),\quad 0\leqslant r_i\leqslant m-1,$$

则我们有

$$b_1\equiv r_1(\mathrm{mod}\, m),\ b_2\equiv r_2(\mathrm{mod}\, m),\cdots,\ b_{\varphi(m)}\equiv r_{\varphi(m)}(\mathrm{mod}\, m).\quad(9)$$

其中$0\leqslant r_1\leqslant m-1$, $0\leqslant r_2\leqslant m-1,\cdots,0\leqslant r_{\varphi(m)}\leqslant m-1$. 由于$b_1,b_2,\cdots,b_{\varphi(m)}$是模$m$的一个简化剩余系, 所以$r_1$, $r_2,\cdots,r_{\varphi(m)}$和$1,a_2,\cdots,a_{\varphi(m)}$只是在次序上可能有不同. 由于在$1,a_2,\cdots,a_{\varphi(m)}$中,任取出二个整数时,这二个整数对模$m$是不同余的,所以在$r_1,r_2,\cdots,r_{\varphi(m)}$中任取出二个整数时,这二个整数对模$m$是不同余的. 故由(9)式知道,在$b_1$, $b_2,\cdots,b_{\varphi(m)}$中任取出二个整数,则这二个整数对模$m$是不同余的. 由于在$1,a_2,\cdots,a_{\varphi(m)}$中,任取出一个整数时,这个整数和$m$是互素的,所以在$r_1,r_2,\cdots,r_{\varphi(m)}$,中,任取出一个整数时,这个整数和$m$是互素的. 故由(9)式和引理9知道,在$b_1,b_2,\cdots,b_{\varphi(m)}$中任取出一个整数时,则这个整数是和$m$互素的.

引理12 设m是一个大于1的整数, $b_1,b_2,\cdots,b_{\varphi(m)}$是$\varphi(m)$个和$m$互素的整数. 又设在$b_1,b_2,\cdots,b_{\varphi(m)}$中任取出二个整数时,这二个整数对模$m$是不同余的, 则$b_1,b_2,\cdots$, $b_{\varphi(m)}$是模m的一个简化剩余系.

证 设$1<a_2<\cdots<a_{\varphi(m)}$是不大于$m$而和$m$互素的全体正整数. 令$r_i$(其中$i=1,2,\cdots,m$)是一个整数,满足条件

$$b_i\equiv r_i(\mathrm{mod}\, m),\quad 0\leqslant r_i\leqslant m-1,$$

则我们有

$$b_1\equiv r_1(\mathrm{mod}\, m),b_2\equiv r_2(\mathrm{mod}\, m),\cdots,b_{\varphi(m)}\equiv r_{\varphi(m)}(\mathrm{mod}\, m).\quad(10)$$

其中 $0\leqslant r_1\leqslant m-1, 0\leqslant r_2\leqslant m-1,\cdots, 0\leqslant r_{\varphi(m)}\leqslant m-1$. 由于在 $b_1, b_2,\cdots, b_{\varphi(m)}$ 中，任取出一个整数时，这个整数和 m 是互素的，故由 (10) 式和引理 9 知道，在 $r_1, r_2,\cdots, r_{\varphi(m)}$ 中任取出一个整数时，则这个整数是和 m 互素的. 由于在 $b_1, b_2,\cdots, b_{\varphi(m)}$ 中任取出二个整数时，这二个整数对模 m 是不同余的，故由 (10) 式知道，在 $r_1, r_2,\cdots, r_{\varphi(m)}$ 中任取出二个整数时，则这二个整数对模 m 是不同余的. 因而 $r_1, r_2,\cdots, r_{\varphi(m)}$ 和 $1, a_2,\cdots, a_{\varphi(m)}$ 只是在次序上可能有不同，即 $b_1, b_2,\cdots, b_{\varphi(m)}$ 是模 m 的一个简化剩余系.

引理 13 设 m 是一个大于 1 的整数，a 是一个整数且满足条件 $(a, m)=1$. 如果 $b_1, b_2,\cdots, b_{\varphi(m)}$ 是模 m 的一个简化剩余系，则

$$ab_1, ab_2,\cdots, ab_{\varphi(m)}$$

也是模 m 的一个简化剩余系.

证 由于引理 11 和 $b_1, b_2,\cdots, b_{\varphi(m)}$ 是模 m 的一个简化剩余系，我们知道在 $b_1, b_2,\cdots, b_{\varphi(m)}$ 中任取出一个整数时，则这个整数和 m 是互素的. 由于 $(a, m)=1$，我们知道在 $ab_1, ab_2,\cdots, ab_{\varphi(m)}$ 中任取出一个整数时，则这个整数和 m 是互素的. 设在 $ab_1, ab_2,\cdots, ab_{\varphi(m)}$ 中存在二个整数 ab_k, ab_λ (其中 $1\leqslant k<\lambda\leqslant\varphi(m)$)，使得

$$ab_k\equiv ab_\lambda \pmod m \tag{11}$$

成立. 由 $(a, m)=1$, (11) 式和引理 2，我们有

$$b_k\equiv b_\lambda \pmod m. \tag{12}$$

由于引理 11 和 $b_1, b_2,\cdots, b_{\varphi(m)}$ 是模 m 的一个简化剩余系，故在 $b_1, b_2,\cdots, b_{\varphi(m)}$ 中任取出二个整数时，这二个整数对模 m 是不同余的，故 (12) 式不成立，从而 (11) 式不成立. 因而在 $ab_1, ab_2,\cdots, ab_{\varphi(m)}$ 中任取出二个整数时，则这二个整数对模 m 是不同余的. 由引理 12 及在 $ab_1, ab_2,\cdots, ab_{\varphi(m)}$ 中任取

出一个整数时，这个整数和m是互素的，得到 $ab_1,ab_2,\cdots,ab_{\varphi(m)}$是模$m$的一个简化剩余系.

§5. 欧拉定理、费尔马定理及其应用

定理 1（欧拉） 设m是一个大于 1 的整数，a 是一个整数且满足条件 $(a,m)=1$，则我们有

$$a^{\varphi(m)}\equiv 1(\bmod m).$$

证 设 $1<a_2<\cdots<a_{\varphi(m)}$ 是不大于m而和m互素的全体正整数. 令 r_1 是一个整数，满足条件

$$a\equiv r_1(\bmod m),\quad 0\leqslant r_1\leqslant m-1.$$

令 r_i（其中 $i=2,\cdots,\varphi(m)$）是一个整数，满足条件

$$aa_i\equiv r_i(\bmod m),\quad 0\leqslant r_i\leqslant m-1,$$

则我们有

$$a\equiv r_1(\bmod m),\ aa_2\equiv r_2(\bmod m),\cdots,aa_{\varphi(m)}\equiv r_{\varphi(m)}(\bmod m). \tag{13}$$

其中 $0\leqslant r_1\leqslant m-1, 0\leqslant r_2\leqslant m-1,\cdots,0\leqslant r_{\varphi(m)}\leqslant m-1$. 由于 $1,a_2,\cdots,a_{\varphi(m)}$ 是模m的一个简化剩余系，并由于 $(a,m)=1$ 和引理 13，我们知道 $a,aa_2,\cdots,aa_{\varphi(m)}$ 是模m的一个简化剩余系，所以 $r_1,r_2,\cdots,r_{\varphi(m)}$ 和 $1,a_2,\cdots,a_{\varphi(m)}$ 只是在次序上可能有不同，故得

$$r_1r_2\cdots r_{\varphi(m)}=a_2\cdots a_{\varphi(m)}. \tag{14}$$

由于(13)式和 $a(aa_2)\cdots(aa_{\varphi(m)})=a^{\varphi(m)}a_2\cdots a_{\varphi(m)}$，我们有

$$a^{\varphi(m)}a_2\cdots a_{\varphi(m)}\equiv r_1r_2\cdots r_{\varphi(m)}(\bmod m). \tag{15}$$

由(14)和(15)式我们有

$$a^{\varphi(m)}a_2\cdots a_{\varphi(m)}\equiv a_2\cdots a_{\varphi(m)}(\bmod m). \tag{16}$$

由于$a_2,\cdots,a_{\varphi(m)}$都是和$m$互素的，所以 $a_2\cdots a_{\varphi(m)}$ 和m互素，故由引理 2 知道可以把 $a_2\cdots a_{\varphi(m)}$ 从(16)式的二边同时消去，所以我们有

$$a^{\varphi(m)} \equiv 1(\mathrm{mod}\ m).$$

定理 2（费尔马） 如果 p 是一个素数，$p\nmid a$，则我们有

$$a^{p-1} \equiv 1(\mathrm{mod}\ p).$$

证 由引理 10 我们有 $\varphi(p) = p - 1$. 由于 p 是一个素数，$p\nmid a$，得到 $(p, a) = 1$. 在定理 1 中取 $m = p$，得到

$$a^{p-1} \equiv 1(\mathrm{mod}\ p).$$

由 $341 = 11 \times 31$，所以 341 不是素数. 由 $1024 = 341 \times 3 + 1$，得到 $1024 \equiv 1(\mathrm{mod}\ 341)$. 由 $2^{340} = (2^{10})^{34} = (1024)^{34}$ 和引理3，得到 $2^{340} \equiv 1(\mathrm{mod}\ 341)$. 所以说，存在一个正整数 m 和一个整数 a，$m\nmid a$，这里 m 不是素数，使得 $a^{m-1} \equiv 1(\mathrm{mod}\ m)$，即定理 2 的逆定理不成立.

例 7 设 a，b，c 都是正整数，如果今天是星期天，请问经过 a^{b^c} 天后是星期几？

解 设 $a = 7m + a_1$，其中 m 和 a_1 都是非负整数且 $a_1 \leqslant 6$. 当 $a_1 = 0$ 时，有 $7|a$，而得到 $7|a^{b^c}$. 故经过 a^{b^c} 天后还是星期天.

现在我们假定 $1 \leqslant a_1 \leqslant 6$. 由 $a = 7m + a_1$ 得到 $a \equiv a_1(\mathrm{mod}\ 7)$. 由引理 3 我们有

$$a^{b^c} \equiv a_1^{b^c}(\mathrm{mod}\ 7). \tag{17}$$

由于 a_1 是一个不大于 6 的正整数，故有 $(a_1, 7) = 1$. 由于 7 是一个素数，故由定理 2 我们有

$$a_1^6 \equiv 1(\mathrm{mod}\ 7). \tag{18}$$

现在设 $b = 6n + b_1$，其中 n 和 b_1 都是非负整数且 $b_1 \leqslant 5$. 由 $b = 6n + b_1$ 我们有

$$b \equiv b_1(\mathrm{mod}\ 6). \tag{19}$$

当 $b_1 = 0$时，由 (19) 式得到 $6|b$，故得 $6|b^c$. 由(18)式和引理 3，我们有 $a_1^{b^c} \equiv 1(\mathrm{mod}\ 7)$，由 (17) 式和引理 1，我们有 $a^{b^c} \equiv 1(\mathrm{mod}\ 7)$. 即经过 a^{b^c} 天后，应该是星期一.

当 $b_1=1$ 时，由(19)式有 $b\equiv 1(\bmod 6)$．由引理3有 $b^c\equiv 1(\bmod 6)$．设 $b^c=6n_1+1$，其中 n_1 是一个非负整数．由(18)式和引理3，我们有 $a_1^{6n_1}\equiv 1(\bmod 7)$．由 $b^c=6n_1+1$ 得到 $a_1^{b^c}\equiv a_1(\bmod 7)$．故由(17)式和引理1，我们有 $a^{b^c}\equiv a_1(\bmod 7)$．即经过 a^{b^c} 天后，应该是星期 a_1．

当 $b_1=2$ 时，由(19)式有 $b\equiv 2(\bmod 6)$．由引理3，有 $b^c\equiv 2^c(\bmod 6)$．现在设 $c=2c_1+1$，其中 c_1 是一个非负整数，这时我们有 $2^c\equiv 2(\bmod 6)$．由 $b^c\equiv 2^c(\bmod 6)$ 和引理1，我们有 $b^c\equiv 2(\bmod 6)$．设 $b^c=6n_1+2$，其中 n_1 是一个非负整数．由(18)式和引理3，我们有 $a_1^{6n_1}\equiv 1(\bmod 7)$．由 $b^c=6n_1+2$，得到 $a_1^{b^c}\equiv a_1^2(\bmod 7)$．故由(17)式和引理1，我们有 $a^{b^c}\equiv a_1^2(\bmod 7)$．我们又有

$$1^2\equiv 1(\bmod 7),\quad 2^2\equiv 4(\bmod 7),\quad 3^2\equiv 2(\bmod 7),$$
$$4^2\equiv 2(\bmod 7),\quad 5^2\equiv 4(\bmod 7),\quad 6^2\equiv 1(\bmod 7).$$

故当 c 是奇正整数，$a_1=1$ 或 $a_1=6$ 时，有 $a^{b^c}\equiv 1(\bmod 7)$．当 c 是奇正整数，$a_1=2$ 或 $a_1=5$ 时，有 $a^{b^c}\equiv 4(\bmod 7)$．当 c 是奇正整数，$a_1=3$ 或 $a_1=4$ 时，有 $a^{b^c}\equiv 2(\bmod 7)$．即当 c 是奇正整数而 $a_1=1$ 或 $a_1=6$ 时，经过 a^{b^c} 天后，应该是星期一．当 c 是奇正整数而 $a_1=2$ 或 $a_1=5$ 时，经过 a^{b^c} 天后，应该是星期四．当 c 是奇正整数而 $a_1=3$ 或 $a_1=4$ 时，经过 a^{b^c} 天后，应该是星期二．当 $c=2c_2+2$，其中 c_2 是一个非负整数时，我们有 $2^c\equiv 4(\bmod 6)$．由 $b^c\equiv 2^c(\bmod 6)$ 和引理1，我们有 $b^c\equiv 4(\bmod 6)$．设 $b^c=6n_2+4$，其中 n_2 是一个非负整数，由(18)式和引理3，我们有 $a_1^{6n_2}\equiv 1(\bmod 7)$．由 $b^c=6n_2+4$ 得到 $a_1^{b^c}\equiv a_1^4(\bmod 7)$．故由(17)式和引理1，我们有 $a^{b^c}\equiv a_1^4(\bmod 7)$．我们又有

$$1^4\equiv 1(\bmod 7),\quad 2^4\equiv 2(\bmod 7),\quad 3^4\equiv 4(\bmod 7),$$
$$4^4\equiv 4(\bmod 7),\quad 5^4\equiv 2(\bmod 7),\quad 6^4\equiv 1(\bmod 7).$$

故当 c 是偶正整数，$a_1=1$ 或 $a_1=6$ 时，有 $a^{b^c}\equiv 1(\bmod 7)$。当 c 是偶正整数，$a_1=2$ 或 $a_1=5$ 时，有 $a^{b^c}\equiv 2(\bmod 7)$。当 c 是偶正整数，$a_1=3$ 或 $a_1=4$ 时，有 $a^{b^c}\equiv 4(\bmod 7)$。即当 c 是偶正整数而 $a_1=1$ 或 $a_1=6$ 时，经过 a^{b^c} 天后，应该是星期一。当 c 是偶正整数而 $a_1=2$ 或 $a_1=5$ 时，经过 a^{b^c} 天后，应该是星期二。当 c 是偶正整数而 $a_1=3$ 或 $a_1=4$ 时，经过 a^{b^c} 天后，应该是星期四。

当 $b_1=3$ 时，由 (19) 式有 $b\equiv 3(\bmod 6)$。由引理 3，有 $b^c\equiv 3^c(\bmod 6)$。由于 c 是一个正整数，我们有 $3^c\equiv 3(\bmod 6)$，故由引理 1 我们有 $b^c\equiv 3(\bmod 6)$。设 $b^c=6n_1+3$，其中 n_1 是一个非负整数。由(18)式和引理3，我们有 $a_1^{6n_1}\equiv 1(\bmod 7)$。由 $b^c=6n_1+3$，得到 $a_1^{b^c}\equiv a_1^3(\bmod 7)$。故由 (17) 式和引理 1，我们有 $a^{b^c}\equiv a_1^3(\bmod 7)$。我们又有

$$1^3\equiv 1(\bmod 7),\quad 2^3\equiv 1(\bmod 7),\quad 3^3\equiv 6(\bmod 7),$$
$$4^3\equiv 1(\bmod 7),\quad 5^3\equiv 6(\bmod 7),\quad 6^3\equiv 6(\bmod 7).$$

即当 $a_1=1,2,4$ 时，有 $a^{b^c}\equiv 1(\bmod 7)$，而当 $a_1=3,5,6$ 时，有 $a^{b^c}\equiv 6(\bmod 7)$。故当 $a_1=1,2,4$ 时，经过 a^{b^c} 天后，应该是星期一，而当 $a_1=3,5,6$ 时，经过 a^{b^c} 天后，应该是星期六。

当 $b_1=4$ 时，由(19)式有 $b\equiv 4(\bmod 6)$。由引理 3，有 $b^c\equiv 4^c(\bmod 6)$。由于 c 是一个正整数，我们有 $4^c\equiv 4(\bmod 6)$，故由引理 1 我们有 $b^c\equiv 4(\bmod 6)$。设 $b^c=6n_1+4$，其中 n_1 是一个非负整数。由 (18) 式和引理 3，我们有 $a_1^{6n_1}\equiv 1(\bmod 7)$。由 $b^c=6n_1+4$，得到 $a_1^{b^c}\equiv a_1^4(\bmod 7)$。故由(17)式和引理 1，我们有 $a^{b^c}\equiv a_1^4(\bmod 7)$。我们又有

$$1^4\equiv 1(\bmod 7),\quad 2^4\equiv 2(\bmod 7),\quad 3^4\equiv 4(\bmod 7),$$
$$4^4\equiv 4(\bmod 7),\quad 5^4\equiv 2(\bmod 7),\quad 6^4\equiv 1(\bmod 7).$$

故当 $a_1=1$ 或 $a_1=6$ 时，有 $a^{b^c}\equiv 1(\bmod 7)$。当 $a_1=2$ 或

$a_1=5$ 时，有 $a^{b^c}\equiv 2(\mathrm{mod}\ 7)$．当 $a_1=3$ 或 $a_1=4$ 时，有 $a^{b^c}\equiv 4(\mathrm{mod}\ 7)$，即当 $a_1=1$ 或 $a_1=6$ 时，经过 a^{b^c} 天后，应该是星期一．当 $a_1=2$ 或 $a_1=5$ 时，经过 a^{b^c} 天后，应该是星期二．当 $a_1=3$ 或 $a_1=4$ 时，经过 a^{b^c} 天后，应该是星期四．

当 $b_1=5$ 时，由 (19) 式有 $b\equiv 5(\mathrm{mod}\ 6)$．由引理 3，有 $b^c\equiv 5^c(\mathrm{mod}\ 6)$．现在设 $c=2c_1+1$，其中 c_1 是一个非负整数，我们有 $5^c\equiv 5(\mathrm{mod}\ 6)$．由 $b^c\equiv 5^c(\mathrm{mod}\ 6)$ 和引理 1，我们有 $b^c\equiv 5(\mathrm{mod}\ 6)$．设 $b^c=6n_1+5$，其中 n_1 是一个非负整数．由 (18) 式和引理 3，我们有 $a_1^{6n_1}\equiv 1(\mathrm{mod}\ 7)$．由 $b^c=6n_1+5$，得到 $a_1^{b^c}\equiv a_1^5(\mathrm{mod}\ 7)$．故由 (17) 式和引理 1，我们有 $a^{b^c}\equiv a_1^5(\mathrm{mod}\ 7)$．我们又有

$$1^5\equiv 1(\mathrm{mod}\ 7),\quad 2^5\equiv 4(\mathrm{mod}\ 7),\quad 3^5\equiv 5(\mathrm{mod}\ 7),$$
$$4^5\equiv 2(\mathrm{mod}\ 7),\quad 5^5\equiv 3(\mathrm{mod}\ 7),\quad 6^5\equiv 6(\mathrm{mod}\ 7).$$

即当 $a_1=1$ 时，经过 a^{b^c} 天后，应该是星期一．当 $a_1=2$ 时，经过 a^{b^c} 天后，应该是星期四．当 $a_1=3$ 时，经过 a^{b^c} 天后，应该是星期五．当 $a_1=4$ 时，经过 a^{b^c} 天后，应该是星期二．当 $a_1=5$ 时，经过 a^{b^c} 天后，应该是星期三．当 $a_1=6$ 时，经过 a^{b^c} 天后，应该是星期六．现在设 $c=2c_2+2$，其中 c_2 是一个非负整数，这时我们有 $5^c\equiv 1(\mathrm{mod}\ 6)$．由 $b^c\equiv 5^c(\mathrm{mod}\ 6)$ 和引理 1，我们有 $b^c\equiv 1(\mathrm{mod}\ 6)$．设 $b^c=6n_1+1$，其中 n_1 是一个非负整数．由(18)式和引理 3，我们有 $a_1^{6n}\equiv 1(\mathrm{mod}\ 7)$．由 $b^c=6n_1+1$，得到 $a_1^{b^c}\equiv a_1(\mathrm{mod}\ 7)$．故由 (17) 式和引理 1，我们有 $a^{b^c}\equiv a_1(\mathrm{mod}\ 7)$．即当 c 是偶正整数时，经过 a^{b^c} 天后，应该是星期 a_1．

例 8 求 $(12371^{56}+34)^{28}$ 被 111 除的余数．

解 由 $12371=111^2+50$，得到 $12371\equiv 50(\mathrm{mod}\ 111)$．由引理 3，我们有

$$12371^{56} \equiv 50^{56} (\mathrm{mod}\ 111). \tag{20}$$

我们又有 $(50)^{28} = (125000)^9(50)$，$125000 \equiv 14 (\mathrm{mod}\ 111)$，故由引理 3，得到

$$(50)^{28} \equiv (14)^9 (50) (\mathrm{mod}\ 111). \tag{21}$$

又由 $14^3 \equiv 80 (\mathrm{mod}\ 111)$，$(80)^3 \equiv 68 (\mathrm{mod}\ 111)$，$(68)(50) \equiv 70 (\mathrm{mod}\ 111)$，得到

$$(50)^{28} \equiv 70 (\mathrm{mod}\ 111). \tag{22}$$

由引理 3，我们有 $(50)^{56} \equiv 70^2 (\mathrm{mod}\ 111)$. 我们又有 $70^2 \equiv 16 (\mathrm{mod}\ 111)$，由 (20) 式得到 $12371^{56} \equiv 16 (\mathrm{mod}\ 111)$. 由引理 3，我们有 $(12371^{56} + 34)^{28} \equiv 50^{28} (\mathrm{mod}\ 111)$. 由 (22) 式得到 $(12371^{56} + 34)^{28} \equiv 70 (\mathrm{mod}\ 111)$. 故得到 $(12371^{56} + 34)^{28}$ 被 111 除的余数是 70.

例 1 的证明 在例 7 中取 $a = 773$，$m = 110$，$a_1 = 3$，$b = 3169$，$n = 528$，$b_1 = 1$. 由例 7 知道如果今天是星期天，则经过 773^{3169^c} 天后，应该是星期三.

引理 14 如果 $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$，其中 $p_1, \cdots, p_n$ 都是素数而 $\alpha_1, \cdots, \alpha_n$ 都是正整数，则我们有

$$\varphi(a) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_n^{\alpha_n - 1}(p_n - 1).$$

证 当 $n = 1$ 时，由引理 10 知道本引理成立. 现在设 $n \geqslant 2$. 不大于 a 的 p_1 的倍数是

$$p_1, 2p_1, \cdots, \frac{a}{p_1} p_1,$$

共有 $\frac{a}{p_1}$ 个. 故不大于 a 而和 p_1 互素的正整数共有

$$a - \frac{a}{p_1} = a\left(1 - \frac{1}{p_1}\right) \tag{23}$$

个. 不大于 a 的 p_2 的倍数是

$$p_2, 2p_2, 3p_2, \cdots, \frac{a}{p_2} p_2,$$

共有 $\frac{a}{p_2}$ 个。但在 $p_2, 2p_2, 3p_2, \cdots, \frac{a}{p_2}p_2$ 中，有 p_1 的倍数，即

$$p_1p_2, 2p_1p_2, 3p_1p_2, \cdots, \frac{a}{p_1p_2}p_1p_2,$$

共有 $\frac{a}{p_1p_2}$ 个．故不大于 a 而只为 p_2 的倍数不同时为 p_1 的倍数的正整数共有

$$\frac{a}{p_2}-\frac{a}{p_1p_2}=\frac{a}{p_2}\left(1-\frac{1}{p_1}\right) \tag{24}$$

个．故不大于 a 而和 p_1，p_2 都是互素的正整数共有

$$a\left(1-\frac{1}{p_1}\right)-\frac{a}{p_2}\left(1-\frac{1}{p_1}\right)=a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \tag{25}$$

个．当 $n=2$ 时，由 $a=p_1^{\alpha_1}p_2^{\alpha_2}$ 和 (25) 式我们有

$$\varphi(a)=p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1).$$

故当 $n=2$ 时本引理成立．现在设 $n\geqslant 3$．不大于 a 的 p_3 的倍数是

$$p_3, 2p_3, 3p_3, \cdots, \frac{a}{p_3}p_3,$$

共有 $\frac{a}{p_3}$ 个．但在 $p_3, 2p_3, 3p_3, \cdots, \frac{a}{p_3}p_3$ 中，有 p_1 的倍数，即

$$p_1p_3, 2p_1p_3, \cdots, \frac{a}{p_1p_3}p_1p_3,$$

共有 $\frac{a}{p_1p_3}$ 个．在 $p_3, 2p_3, 3p_3, \cdots, \frac{a}{p_3}p_3$ 中，有 p_2 的倍数，即

$$p_2p_3, 2p_2p_3, \cdots, \frac{a}{p_2p_3}p_2p_3,$$

共有 $\frac{a}{p_2p_3}$ 个．在 $p_1p_3, 2p_1p_3, \cdots, \frac{a}{p_1p_3}p_1p_3$ 中，有 p_2 的倍数，即

$$p_1p_2p_3, 2p_1p_2p_3, \cdots, \frac{a}{p_1p_2p_3}p_1p_2p_3,$$

共有 $\frac{a}{p_1p_2p_3}$ 个．在 $p_2p_3, 2p_2p_3, \cdots, \frac{a}{p_2p_3}p_2p_3$ 中，有 p_1 的倍数，即

$$p_1p_2p_3, 2p_1p_2p_3, \cdots, \frac{a}{p_1p_2p_3}p_1p_2p_3,$$

共有 $\frac{a}{p_1p_2p_3}$ 个．故不大于 a 而只为 p_3 的倍数并且和 p_1, p_2 都是互素的正整数共有

$$\frac{a}{p_3}-\frac{a}{p_1p_3}-\frac{a}{p_2p_3}+\frac{a}{p_1p_2p_3}=\frac{a}{p_3}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \tag{26}$$

个．由(25)式和(26)式知道，不大于 a 而和 p_1, p_2, p_3 都是互素的正整数共有

$$\begin{aligned} &a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)-\frac{a}{p_3}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \\ &\quad=a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right) \end{aligned} \tag{27}$$

个．当 $n=3$ 时，由 $a=p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}$ 和(27)式我们有

$$\varphi(a)=p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)p_3^{\alpha_3-1}(p_3-1).$$

故当 $n=3$ 时本引理成立．当 $n\geqslant 4$ 时，可用同样方法做下去．我们最后必得到，不大于 a 而和 $p_1, p_2, \cdots, p_n$ 都是互素的正整数(也就是不大于 a 而和 a 互素的正整数)共有

$$a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_n}\right)$$

个．即 $\varphi(a)=p_1^{\alpha_1-1}(p_1-1)\cdots p_n^{\alpha_n-1}(p_n-1)$.

例 9 $3^{8232010}-59049$ 能被 24010000 整除．

证 由 $24010000=2^4 5^4 7^4$ 和引理 14，我们有 $\varphi(24010000)=2^3\times 5^3\times 4\times 7^3\times 6=8232000$．故由定理 1 我们有

$$3^{8232000}\equiv 1(\bmod 24010000). \tag{28}$$

由 (28) 式我们有

$$3^{8232010} - 59049 \equiv 3^{10} - 59049 \pmod{24010000}. \qquad (29)$$

由 $3^{10} = 59049$ 和 (29) 式我们知道例 9 成立.

例 2 的证明 由 $(70, 111) = 1$ 和例 8 中的 $(12371^{56} + 34)^{28} \equiv 70 \pmod{111}$，得到 $(12371^{56} + 34, 111) = 1$. 由于 $111 = 3 \times 37$ 和引理 14，我们有 $\varphi(111) = 2 \times 36 = 72$. 由于 c 是一个正整数并由于定理 1，我们有 $(12371^{56} + 34)^{72c} \equiv 1 \pmod{111}$. 故得到

$$(12371^{56} + 34)^{72c+28} \equiv 70 \pmod{111}.$$

例 10 设 n 是一个正整数而 p 是一个素数，请证明

$$1 + \varphi(p) + \cdots + \varphi(p^n) = p^n. \qquad (30)$$

证 由引理 10 我们有 $1 + \varphi(p) = 1 + p - 1 = p$，故当 $n = 1$ 时，(30) 式成立. 现设 $n \geqslant 2$，由引理 10 我们有

$$\begin{aligned} &1 + \varphi(p) + \cdots + \varphi(p^n) \\ &= 1 + p - 1 + \cdots + p^{n-1}(p - 1) = p^n. \end{aligned}$$

习　　题

1. 设 m_1, m_2 是互素的两个正整数，则当 x_1, x_2 分别通过模 m_1, m_2 的完全剩余系时，$m_2x_1 + m_1x_2$ 通过模 m_1m_2 的完全剩余系.

2. 设 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数，则当 $x_1, x_2, \cdots, x_k$ 分别通过模 $m_1, m_2, \cdots, m_k$ 的完全剩余系时，$M_1x_1 + M_2x_2 + \cdots + M_kx_k$ 通过模 $m_1m_2\cdots m_k$ 的完全剩余系. 这里的 $M_1, M_2, \cdots, M_k$ 由下式定义:

$$m_1m_2\cdots m_k = m_1M_1 = m_2M_2 = \cdots = m_kM_k.$$

3. 设 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数，则当 $x_1, x_2, \cdots, x_k$ 分别通过模 $m_1, m_2, \cdots, m_k$ 的完全剩余系时，$x_1 + m_1x_2 + m_1m_2x_3 + \cdots + m_1m_2\cdots m_{k-1}x_k$ 通过模 $m_1m_2\cdots$

m_k 的完全剩余系。

4. 证明欧拉函数的下列性质:

(i) 若 $N > 2$，则 $\varphi(N)$ 必定是偶数。

(ii) 假若 $(a, b) = 1$，则有 $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

5. 设 $N > 1$，证明: 不大于N且与N互素的所有正整数的和是$\frac{1}{2} N \cdot \varphi(N)$.

6. 假设$m > 1$是正整数，$(a, m) = 1$，又假定$b_1, b_2, \cdots, b_{\varphi(m)}$是模$m$的一个简化剩余系，而 $ab_i = r_i \pmod m$ $(0 \leqslant r_i < m,\ 1 \leqslant i \leqslant \varphi(m))$，则

$$\frac{1}{m}(r_1 + r_2 + \cdots + r_{\varphi(m)}) = \frac{1}{2}\varphi(m).$$

7. 设 $m_1, m_2, \cdots, m_k$ 是k个两两互素的正整数，则当$x_1, x_2, \cdots, x_k$ 分别通过模 $m_1, m_2, \cdots, m_k$ 的简化剩余系时，$M_1x_1 + M_2x_2 + \cdots + M_kx_k$ 通过模 $m_1m_2\cdots m_k$ 的简化剩余系。这里的 $M_1, M_2, \cdots, M_k$ 由下式定义:

$$m_1M_1 = m_2M_2 = \cdots = m_kM_k = m_1m_2\cdots m_k.$$

8. (i) 设 $N = 9450$，求 $\varphi(N)$.

(ii) 求不大于9450且与9450互素的全体正整数的和。

9. (i) 判断 $121^6 - 1$ 能否被 21 整除.

(ii) 求 8^{4965} 除以 13 后的余数.

(iii) 设p是除2和5以外的任一素数，试证:

$p \mid \underbrace{99\cdots9}_{(p-1)k\text{个}}$，$k$是任意正整数。

10. 我们称 $F_n = 2^{2^n} + 1$ 为费尔马数，试证 $641 \mid F_5$.

11. 假设p是素数，a和b是任意二个整数，则有

$$(a + b)^p \equiv a^p + b^p \pmod p.$$

12. 求正整数n和 m，$n > m \geqslant 1$，使得 1978^n 与 1978^m 的最后三位数相等，并且使 $n + m$ 为最小。(第20届国际中

学生数学竞赛题）

13. 设手表上的指针都从12点钟开始走，当分针转过了 a^{b^c} 圈后(其中 a, b, c 都是正整数)，问这时手表的指针指的是几点钟？

第六章　小数、分数和实数

§1. 分数化小数

在本章中我们假定分数中的分子和分母都是正整数．我们可以把分数分成为下列三种：

(1) 真分数．分子小于分母的分数，它们都大于 0 而小于 1．大于 0 而小于 1 的分数叫作真分数．

例如 $\frac{3}{8}$, $\frac{1}{2}$, $\frac{4}{7}$, $\frac{12}{37}$, $\frac{23}{74}$, $\frac{97}{100}$, $\frac{999}{1000}$, ……，这些分数的分子小于分母，因而它们都小于 1，所以都是真分数．

(2) 假分数．分子等于分母或分子大于分母的分数，它们等于 1 或大于 1．等于 1 或大于 1 的分数叫作假分数．

例如 $\frac{5}{3}$, $\frac{1011}{1000}$, $\frac{3}{2}$, $\frac{4}{4}$, $\frac{4}{3}$, $\frac{111}{100}$, $\frac{1001}{1000}$, ……，这些分数都是假分数．

(3) 带分数．整数后面带有分数叫作带分数．

例如 $3\frac{1}{4}$, $11\frac{2}{5}$, $105\frac{4}{5}$, $110\frac{3}{7}$, ……，这些分数都是带分数．

现在我们要来讨论将分数化成小数的问题．因为假分数等于整数或整数加真分数，而带分数等于整数加真分数，所以我们将只讨论真分数．设 $\frac{a}{b}$ 是真分数，则 $0 < a < b$．当 $(a, b) = 1$ 时，则 $\frac{a}{b}$ 叫作既约真分数．当 $\frac{a}{b}$ 不是既约真分数时，则有 $(a, b) = d > 1$，这时存在正整数 a_1, b_1 使得 $a = a_1d$, $b = b_1d$,

$(a_1, b_1) = 1$ 而有 $\frac{a}{b} = \frac{a_1}{b_1}$. 因而任何一个真分数都可以化成为既约真分数，所以我们将只讨论既约真分数.

由于 $1, 2, \cdots, p-1$ 都是和 p 互素的，所以以素数 p 作分母的所有真分数都是既约真分数. 设 b 是一个大于 1 的正整数，由于不大于 b 而和 b 互素的正整数有 $\varphi(b)$ 个，故以 b 为分母的既约真分数共计有 $\varphi(b)$ 个.

有些既约真分数能够化成为有限小数，例如

$$\frac{1}{4} = 0.25, \ \frac{1}{3125} = 0.00032, \ \frac{1}{1024} = 0.0009765625,$$

$$\frac{97}{15625} = 0.006208, \ \frac{3947}{4096} = 0.963623046875.$$

可是有些既约真分数不能够化成为有限小数，例如

$$\frac{4}{9} = 0.44444\cdots, \ \frac{8}{15} = 0.533333\cdots, \ \frac{1}{3} = 0.33333\cdots.$$

引理 1 设 a, b 都是正整数，$a < b$ 而 $(a, b) = 1$. 如果存在一个素数 p，它使得 $p|b$ 但是 $p\nmid 10$，则 $\frac{a}{b}$ 一定不能够化成为有限小数. 如果 $b = 2^{\alpha}5^{\beta}$，其中 α, β 都是非负整数，则 $\frac{a}{b}$ 能够化成为有限小数.

证 如果存在一个素数 p，它使得 $p|b$ 但是 $p\nmid 10$，且 $\frac{a}{b}$ 能够化成为有限小数. 由于 $a < b$ 而得到

$$\frac{a}{b} = 0.a_1a_2\cdots a_n.$$

其中 $a_1, a_2, \cdots, a_n$ 都是不大于 9 的非负整数，但是 $a_n > 0$. 我们又有

$$10^n a = (10^{n-1}a_1 + \cdots + a_n)b. \qquad (1)$$

由于 $(a, b) = 1$，$10^{n-1}a_1 + \cdots + a_n$ 是一个正整数和 (1)

式而得到$b|10^n$. 由于假设$p|b$,所以有$p|10$,这和假设$p\nmid 10$发生矛盾,所以$\frac{a}{b}$不能够化成为有限小数.

设$b=2^{\alpha}5^{\beta}$,其中$\alpha\geqslant\beta\geqslant 0$,则有$\frac{10^{\alpha}a}{b}=5^{\alpha-\beta}a$.由于$\alpha\geqslant\beta\geqslant 0$,所以$5^{\alpha-\beta}a$是一个正整数,我们把$5^{\alpha-\beta}a$记作$d$,则有$\frac{a}{b}=\frac{d}{10^{\alpha}}$. 由于$d$是一个正整数,因而$\frac{d}{10^{\alpha}}$是一个有限小数,所以$\frac{a}{b}$能够化成为有限分数. 设$b=2^{\alpha}5^{\beta}$,其中$\beta>\alpha\geqslant 0$,则有$\frac{10^{\beta}a}{b}=2^{\beta-\alpha}a$. 由于$\beta>\alpha\geqslant 0$,所以$2^{\beta-\alpha}a$是一个正整数. 我们把$2^{\beta-\alpha}a$记作$d_1$,则有$\frac{a}{b}=\frac{d_1}{10^{\beta}}$. 由于$d_1$是一个正整数,因而$\frac{d_1}{10^{\beta}}$是一个有限小数,所以$\frac{a}{b}$能够化成为有限小数.

定义 1 设a_i(其中$i=1, 2, 3,\cdots$)是一个不大于 9 的非负整数. 如果在$0.a_1a_2a_3\cdots a_n\cdots$中任取出一个$a_j$,那么一定存在一个大于$j$的正整数$k$,使得$a_k\neq 0$. 那么我们把$0.a_1a_2a_3\cdots a_n\cdots$叫作一个无限小数.

例如$\frac{7}{22}=0.318181818\cdots$, $\frac{5}{7}=0.7142857142\cdots$.

定义 2 如果对于一个无限小数$0.a_1a_2a_3\cdots a_n\cdots$,能找出二个整数$s\geqslant 0$, $t\geqslant 0$使得

$$a_{s+i}=a_{s+kt+i},\quad i=1, 2,\cdots, t,\quad k=0, 1, 2,\cdots$$

成立,那么我们就称$0.a_1a_2a_3\cdots a_n\cdots$为循环小数,并把$0.a_1a_2a_3\cdots a_n\cdots$简单地记作$0.a_1a_2\cdots a_s\dot{a}_{s+1}\cdots\dot{a}_{s+t}$.

对于循环小数而言,具有上述性质的s及t是不只一个的. 如果找到的t是最小的,那么我们就称$a_{s+1}, a_{s+2},\cdots$,

a_{s+t} 为循环节；t 称为循环节的长度；如果最小的 $s=0$，那循环小数就叫作纯循环小数．如果 $s\geqslant 1$（这里是最小的 s），这时那循环小数就叫作混循环小数．

例 1 求证 $\frac{4}{9}=0.\dot{4}$，$\frac{8}{15}=0.5\dot{3}$，$\frac{3}{14}=0.2\dot{1}4285\dot{7}$．

证 由于 $\frac{4}{9}=0.44444\cdots$，所以有 $\frac{4}{9}=0.\dot{4}$．

由于 $\frac{80}{15}=\frac{16}{3}=5+\frac{1}{3}=5.33333\cdots$，所以有 $\frac{8}{15}=0.533333\cdots$，即 $\frac{8}{15}=0.5\dot{3}$．由于 $\frac{30}{14}=\frac{15}{7}=2+\frac{1}{7}=2.1428571428571\cdots$，所以有 $\frac{3}{14}=0.21428571428571\cdots$，即 $\frac{3}{14}=0.2\dot{1}4285\dot{7}$．

引理 2 设 $0<a<b$，且 $(a,b)=1$．如果 $\frac{a}{b}$ 能表成纯循环小数，则我们有 $(b,10)=1$．

证 设 $\frac{a}{b}$ 能表成纯循环小数，则由 $0<\frac{a}{b}<1$ 及定义 2，我们有

$$\frac{a}{b}=0.a_1\cdots a_ta_1\cdots a_ta_1\cdots a_t\cdots. \tag{2}$$

其中 $a_1,\cdots,a_t$ 都是不大于 9 的非负整数，但是在 $a_1,\cdots,a_t$ 中至少有一个 $a_i\geqslant 1$．因而

$$\frac{10^ta}{b}=10^{t-1}a_1+\cdots+a_t+0.a_1\cdots a_ta_1\cdots a_ta_1\cdots a_t\cdots. \tag{3}$$

由 (3) 式减 (2) 式得到

$\frac{10^ta}{b}-\frac{a}{b}=10^{t-1}a_1+\cdots+a_t$，故得到

$$a(10^t-1)=b(10^{t-1}a_1+\cdots+a_t). \tag{4}$$

由 $10^{t-1}a_1+\cdots+a_t$ 是一个正整数，$(a,b)=1$ 和 (4) 式，

得到

$$10^t - 1 = bm, \tag{5}$$

其中 m 是一个整数．由 $(b, 1)=1$ 和(5)式我们有 $(b, 10^t) = 1$，因而 $(b, 10) = 1$.

引理 3 设 $0 < a < b$ 且 $(a, b) = 1$．令 h 是一个最小的正整数，能使

$$10^h \equiv 1 \pmod b$$

成立，则 $\frac{a}{b}$ 能表成纯循环小数 $0.\dot{a}_1\cdots\dot{a}_h$.

证 由 $10^h \equiv 1 \pmod b$ 得到 $10^h a \equiv a \pmod b$．由 $10^h a - a = bm$，其中 m 是一个整数，得到 $\frac{10^h a}{b} - \frac{a}{b} = m$．设 $\frac{a}{b} = 0.a_1a_2\cdots a_h a_{h+1} a_{h+2}\cdots$，则有 $\frac{10^h a}{b} = 10^{h-1}a_1 + \cdots + a_h + 0.a_{h+1}a_{h+2}a_{h+3}\cdots$，故得到

$$m = 10^{h-1}a_1 + \cdots + a_h.$$

$$0.a_{h+1}a_{h+2}a_{h+3}\cdots = 0.a_1a_2\cdots a_h a_{h+1} a_{h+2}\cdots. \tag{6}$$

由 (6) 式我们有

$$\begin{aligned}
&a_{h+1} = a_1,\\
&a_{h+2} = a_2,\\
&\cdots\cdots\cdots,\\
&a_{2h} = a_h,\\
&a_{2h+1} = a_{h+1} = a_1,\\
&a_{2h+2} = a_{h+2} = a_2,\\
&\cdots\cdots\cdots\cdots.
\end{aligned}$$

引理 4 设 b 是一个正整数且 $(10, b) = 1$．令 h 是一个最小的正整数，能使

$$10^h \equiv 1 \pmod b \tag{7}$$

成立,则有 $h|\varphi(b)$.

证 由 $(10, b)=1$ 和第五章定理 1, 我们有

$$10^{\varphi(b)} \equiv 1 \pmod b. \tag{8}$$

由 h 的定义和(8)式, 我们有 $0<h\leqslant\varphi(b)$. 设 $\varphi(b)=hm+r$, 其中 r 是一个小于 h 的非负整数而 m 是一个正整数. 由(7)式和第五章引理 3, 我们有

$$10^{hm} \equiv 1 \pmod b. \tag{9}$$

由于 $\varphi(b)=hm+r$, 并由(8)和(9)式我们有 $10^r\equiv 1 \pmod b$, 如果 $r=0$, 则有 $h|\varphi(b)$. 如果 $0<r<h$, 则由 $10^r\equiv 1 \pmod b$, (7) 式而和 h 的定义发生矛盾. 故本引理得证.

例 2 设 a 是一个不大于 6 的正整数,请将 $\frac{a}{7}$ 表成为纯循环小数.

解 由于 $(a, 7)=1$, $\varphi(7)=6$,

$$10 \equiv 3 \pmod 7,$$
$$10^2 \equiv 2 \pmod 7,$$
$$10^3 \equiv 6 \pmod 7,$$
$$10^6 \equiv 1 \pmod 7,$$

及引理 4 我们有 $h=6$. 又由引理 3 我们有 $\frac{a}{7}=0.\dot{a}_1a_2a_3a_4a_5\dot{a}_6$, 故得到

$$\frac{1}{7}=0.\dot{1}4285\dot{7}, \qquad \frac{2}{7}=0.\dot{2}8571\dot{4},$$

$$\frac{3}{7}=0.\dot{4}2857\dot{1}, \qquad \frac{4}{7}=0.\dot{5}7142\dot{8},$$

$$\frac{5}{7}=0.\dot{7}1428\dot{5}, \qquad \frac{6}{7}=0.\dot{8}5714\dot{2}.$$

例 3 设 a 是一个不大于 12 的正整数,请将 $\frac{a}{13}$ 表成为纯

循环小数.

解 $(a, 13)=1$，$\varphi(13)=12$，由于

$$10 \equiv 10 \pmod{13}, \quad 10^2 \equiv 9 \pmod{13},$$
$$10^3 \equiv 12 \pmod{13}, \quad 10^4 \equiv 3 \pmod{13},$$
$$10^6 \equiv 1 \pmod{13},$$

及引理 4 我们有 $h=6$. 又由引理 3 我们有 $\frac{a}{13}=0.\dot{a}_1a_2a_3a_4a_5\dot{a}_6$，故得到

$$\frac{1}{13}=0.\dot{0}7692\dot{3}, \quad \frac{2}{13}=0.\dot{1}5384\dot{6},$$
$$\frac{3}{13}=0.\dot{2}3076\dot{9}, \quad \frac{4}{13}=0.\dot{3}0769\dot{2},$$
$$\frac{5}{13}=0.\dot{3}8461\dot{5}, \quad \frac{6}{13}=0.\dot{4}6153\dot{8},$$
$$\frac{7}{13}=0.\dot{5}3846\dot{1}, \quad \frac{8}{13}=0.\dot{6}1538\dot{4},$$
$$\frac{9}{13}=0.\dot{6}9230\dot{7}, \quad \frac{10}{13}=0.\dot{7}6923\dot{0},$$
$$\frac{11}{13}=0.\dot{8}4615\dot{3}, \quad \frac{12}{13}=0.\dot{9}2307\dot{6}.$$

例 4 设 a 是任一个不大于 3988 的正整数，求证 $\frac{a}{3989}$ 是一个纯循环小数，它的循环节不小于 997 位(即 $\frac{a}{3989}=0.\dot{a}_1a_2a_3\cdots\dot{a}_n$，则有 $n \geqslant 997$).

证 由于 3989 是一个素数及 a 是一个不大于 3988 的正整数，所以有 $(a, 3989)=1$. 令 n 是一个最小的正整数，能使

$$10^n \equiv 1 \pmod{3989} \qquad (10)$$

成立．由于 $\varphi(3989)=3988$ 和引理4，我们有 $n|3988$．由于

$$10\equiv 10 \pmod{3989},\quad 10^2\equiv 100 \pmod{3989},$$
$$10^4\equiv 2022 \pmod{3989},$$

所以有 $4\neq n$．由于997是一个素数，$3988=4\times 997$，$4\neq n$，且 $n|3988$，所以有 $n\geqslant 997$．由第五章定理2我们有 $a^{3988}\equiv 1 \pmod{3989}$．故由引理3我们有 $\frac{a}{3989}=0.\dot{a}_1a_2a_3\cdots\dot{a}_n$，其中 $n\geqslant 997$，故例4得证．

我们又有 $\frac{1}{3989}=0.00025068939583855653045\cdots$．

现在我们还有这样一个问题：如果在分母 b 内不光有素因数2，或5，或2及5，而且还有其他的素因数，那么既约分数 $\frac{a}{b}$ 化成小数后，情况又怎样呢？这个问题的答案将由下列引理作出．

引理5 设 a, b, b_1，都是正整数，$a<b$，$(a, b)=1$，$b_1>1$，$(b_1, 10)=1$，$b=2^\alpha 5^\beta b_1$，其中 α, β 都是非负整数但不同时为0．令 h 是一个最小的正整数且能使

$$10^h\equiv 1 \pmod{b_1},$$

则当 $\alpha\geqslant\beta$ 时我们有

$$\frac{a}{b}=0.a_1\cdots a_\alpha\dot{a}_{\alpha+1}\cdots\dot{a}_{\alpha+h};$$

而当 $\alpha<\beta$ 时我们有

$$\frac{a}{b}=0.a_1\cdots a_\beta\dot{a}_{\beta+1}\cdots\dot{a}_{\beta+h}.$$

证 设 $\alpha\geqslant\beta$．我们用 10^α 乘 $\frac{a}{b}$ 得到

$$\frac{10^\alpha a}{b}=\frac{10^\alpha a}{2^\alpha 5^\beta b_1}=\frac{5^{\alpha-\beta}a}{b_1}. \tag{11}$$

因为 $(a, b)=1$ 得到 $(a, b_1)=1$. 因为 $(10, b_1)=1$ 得到 $(5^{\alpha-\beta}, b_1)=1$. 由 $(a, b_1)=1$, $(5^{\alpha-\beta}, b_1)=1$, 所以有

$$(5^{\alpha-\beta}a, b_1)=1. \tag{12}$$

设 $5^{\alpha-\beta}a<b_1$, 则由(12)式, $10^h\equiv 1 \pmod{b_1}$和引理3我们有

$$\frac{5^{\alpha-\beta}a}{b_1}=0.\dot{c}_1\cdots\dot{c}_h.$$

故由(11)式我们有

$$\frac{a}{b}=0.a_1\cdots a_\alpha\dot{a}_{\alpha+1}\cdots\dot{a}_{\alpha+h},$$

其中 $a_1=\cdots=a_\alpha=0$ 而 $a_{\alpha+1}=c_1,\cdots,a_{\alpha+h}=c_h$.

现在设 $5^{\alpha-\beta}a>b_1$. 由(12)式我们有

$$5^{\alpha-\beta}a=b_1q+a_1, \tag{13}$$

其中 q 是一个正整数而 a_1 是一个不大于 b_1-1 的正整数.设 $(a_1,b_1)=d>1$, 则由(13)式有 $d|5^{\alpha-\beta}a$. 由于 $d|b_1$, $d|5^{\alpha-\beta}a$, $d>1$, 这和(12)式发生矛盾,故 $(a_1, b_1)=1$. 由于 h 是一个最小的正整数且能使 $10^h\equiv 1 \pmod{b_1}$; 由 $0<a_1<b_1$, $(a_1, b_1)=1$ 和引理3我们有

$$\frac{a_1}{b_1}=0.\dot{c}_1\cdots\dot{c}_h. \tag{14}$$

由(11)和(13)式我们有

$$\frac{10^\alpha a}{b}=q+\frac{a_1}{b_1}. \tag{15}$$

由于 $1\leqslant a<b$, $1\leqslant a_1<b_1$ 和(15)式我们有 $1\leqslant q\leqslant 10^\alpha$. 故由(14)和(15)式我们有

$$\frac{a}{b}=\frac{q+\dfrac{a_1}{b_1}}{10^\alpha}=0.a_1\cdots a_\alpha\dot{a}_{\alpha+1}\cdots\dot{a}_{\alpha+h},$$

其中 $a_{\alpha+1}=c_1,\cdots,a_{\alpha+h}=c_h$. 故当 $\alpha\geqslant\beta$ 时本引理成立.

现在设 $\alpha<\beta$. 我们用 10^{β} 乘 $\frac{a}{b}$ 得到

$$\frac{10^{\beta}a}{b}=\frac{10^{\beta}a}{5^{\beta}2^{\alpha}b_1}=\frac{2^{\beta-\alpha}a}{b_1}. \tag{16}$$

因为 $(a, b)=1$ 得到 $(a, b_1)=1$. 因为 $(10, b_1)=1$ 得到 $(2^{\beta-\alpha}, b_1)=1$. 由 $(a, b_1)=1$, $(2^{\beta-\alpha}, b_1)=1$ 得到

$$(2^{\beta-\alpha}a, b_1)=1. \tag{17}$$

设 $2^{\beta-\alpha}a<b_1$, 则由于 h 是一个最小的正整数且能使 $10^h\equiv 1 \pmod{b_1}$ 成立,并由于(17)式和引理3,我们有

$$\frac{2^{\beta-\alpha}a}{b_1}=0.\dot{g}_1\cdots\dot{g}_h. \tag{18}$$

故由(16)和(18)式我们有

$$\frac{a}{b}=0.a_1\cdots a_{\beta}\dot{a}_{\beta+1}\cdots\dot{a}_{\beta+h},$$

其中

$$a_1=\cdots=a_{\beta}=0, \text{ 而 } a_{\beta+1}=g_1, \cdots, a_{\beta+h}=g_h.$$

现在设 $2^{\beta-\alpha}a>b_1$, 则由(17)式我们有

$$2^{\beta-\alpha}a=b_1m+a_1, \tag{19}$$

其中 m 是一个正整数而 a_1 是一个不大于 b_1-1 的正整数. 设 $(a_1, b_1)=d>1$, 则由(19)式有 $d\mid 2^{\beta-\alpha}a$. 由于 $d\mid b_1$, $d\mid 2^{\beta-\alpha}a$, $d>1$, 这和(17)式发生矛盾,故有 $(a_1, b_1)=1$. 由于 h 是一个最小的正整数且能使 $10^h\equiv 1 \pmod{b_1}$成立,由 $0<a_1<b_1$,$(a_1, b_1)=1$ 和引理 3 我们有

$$\frac{a_1}{b_1}=0.\dot{g}_1\cdots\dot{g}_h. \tag{20}$$

由(16)和(19)式我们有

$$\frac{10^{\beta}a}{b}=m+\frac{a_1}{b_1}. \tag{21}$$

由于 $1\leqslant a<b$, $1\leqslant a_1<b_1$ 和(21)式, 我们有 $1\leqslant m<$

10^β,故由(20)和(21)式我们有

$$\frac{a}{b}=\frac{m+\dfrac{a_1}{b_1}}{10^\beta}=0.a_1\cdots a_\beta\dot{a}_{\beta+1}\cdots\dot{a}_{\beta+h},$$

其中 $a_{\beta+1}=g_1,\cdots,a_{\beta+h}=g_h$. 故当 $\alpha<\beta$ 时本引理也成立,引理得证.

例 5 请把 $\frac{15}{308}$ 化成小数.

解 由于 $308=4\times 77=2^2\cdot 77$, $\varphi(77)=(11-1)\times(7-1)=60$.

又有

$$10\equiv 10\pmod{77},\qquad 10^2\equiv 23\pmod{77},$$
$$10^3\equiv 76\pmod{77},\qquad 10^4\equiv 67\pmod{77},$$
$$10^5\equiv 54\pmod{77},\qquad 10^6\equiv 1\pmod{77},$$

所以可在引理 5 中取 $a=15$, $b=308$, $\alpha=2$, $\beta=0$, $h=6$, $b_1=77$. 由引理 5 我们有 $\frac{15}{308}=0.a_1a_2\dot{a}_3a_4\cdots\dot{a}_8$,经过计算我们有

$$\frac{15}{308}=0.04\dot{8}7012\dot{9}.$$

例 6 请把 $\frac{1}{17408}$ 化成小数.

解 由于 $17408=1024\times 17=2^{10}\cdot 17$, $\varphi(17)=16$.

又有

$$10\equiv 10\pmod{17},\qquad 10^2\equiv 15\pmod{17},$$
$$10^4\equiv 4\pmod{17},\qquad 10^8\equiv 16\pmod{17},$$
$$10^{16}\equiv 1\pmod{17},$$

所以可在引理 5 中取 $a=1$, $b=17408$, $\alpha=10$, $\beta=0$,

$h=16$，$b_1=17$. 由引理 5 我们有 $\dfrac{1}{17408}=0.a_1a_2\cdots a_{10}\dot{a}_{11}$ $a_{12}\cdots\dot{a}_{26}$，经过计算我们有

$$\frac{1}{17408}=0.0000574448\dot{5}29411764705882\dot{3}.$$

§2. 小数化分数

有限小数都能够化成为分数. 设

$$0.a_1a_2\cdots a_n$$

是一个有限小数，其中 $a_i(i=1,2,\cdots,n)$ 都是不大于 9 的非负整数，但是 $a_n\geqslant 1$. 我们有

$$0.a_1a_2\cdots a_n=\frac{10^{n-1}a_1+10^{n-2}a_2+\cdots+a_n}{10^n}. \quad (22)$$

设 $(10^{n-1}a_1+10^{n-2}a_2+\cdots+a_n,\ 10^n)=d$，则我们有

$$10^{n-1}a_1+10^{n-2}a_2+\cdots+a_n=da,\quad 10^n=db,$$

其中 a，b 都是正整数且 $(a,b)=1$，$a<b$. 由 (22) 式我们有

$$0.a_1a_2\cdots a_n=\frac{a}{b},$$

其中 $\dfrac{a}{b}$ 是一个既约真分数.

纯循环小数都能够化成为分数. 设

$$0.\dot{a}_1\cdots\dot{a}_t$$

是一个循环节等于 t 的纯循环小数，其中 $a_i(i=1,2,\cdots,t)$ 都是不大于 9 的非负整数，但是在 $a_1,\cdots,a_t$ 中至少有一个是正整数. 令 $A=0.\dot{a}_1\cdots\dot{a}_t$，由于 $A=0.a_1\cdots a_ta_1\cdots a_ta_1\cdots a_t\cdots$，所以我们有

$$\begin{aligned}10^tA&=10^{t-1}a_1+10^{t-2}a_2+\cdots+a_t+0.a_1\cdots a_ta_1\cdots a_t\cdots\\&=a+A,\end{aligned}\quad (23)$$

其中 $a=10^{t-1}a_1+10^{t-2}a_2+\cdots+a_t$ 是一个正整数． 令 $b=10^t-1$，则由于 $t\geqslant 1$，所以 b 是一个正整数． 由(23)式我们有

$$A=\frac{a}{10^t-1},$$

即 $0.\dot{a}_1\cdots\dot{a}_t=\dfrac{a}{b}$.

混循环小数也都能够化成为分数．设

$$0.a_1\cdots a_s\dot{a}_{s+1}\cdots\dot{a}_{s+t}$$

是一个混循环小数．我们有

$$0.a_1\cdots a_s\dot{a}_{s+1}\cdots\dot{a}_{s+t}=0.a_1\cdots a_s+\frac{0.\dot{a}_{s+1}\cdots\dot{a}_{s+t}}{10^s}. \tag{24}$$

由于 $0.a_1\cdots a_s$ 是一个有限小数，所以有

$$0.a_1\cdots a_s=\frac{a}{b}. \tag{25}$$

其中 a, b 都是正整数，$(a, b)=1$, $a<b$.由于 $0.\dot{a}_{s+1}\cdots\dot{a}_{s+t}$ 是一个纯循环小数，所以有

$$0.\dot{a}_{s+1}\cdots\dot{a}_{s+t}=\frac{c}{d}, \tag{26}$$

其中 c, d 都是正整数．由(24)到(26)式我们有

$$0.a_1\cdots a_s\dot{a}_{s+1}\cdots\dot{a}_{s+t}=\frac{a}{b}+\frac{c}{10^s d}=\frac{10^s ad+bc}{10^s bd}.$$

引理 6 设 $0.a_1a_2a_3\cdots a_n\cdots$ 不能够化成为有限小数，也不能够化成为循环小数，则 $0.a_1a_2a_3\cdots a_n\cdots$ 不能够化成为分数．

证 如果存在二个正整数 a, b，使得

$$0.a_1a_2a_3\cdots a_n\cdots=\frac{a}{b} \tag{27}$$

成立，则有 $0<a<b$．设 $(a, b)=d$，则有 $a=da_1$, $b=db_1$．其中 $(a_1, b_1)=1$, $0<a_1<b_1$．由(27)式我们有

$$0.a_1a_2a_3\cdots a_n\cdots=\frac{a}{b}=\frac{a_1d}{b_1d}=\frac{a_1}{b_1}. \qquad (28)$$

设 $(b_1, 10)=1$，则由 $0<a_1<b_1$，$(a_1, b_1)=1$，(28)式，引理 3 和引理 4 知道 $0.a_1a_2\cdots a_n\cdots$ 能化成为循环小数，这和假设 $0.a_1a_2a_3\cdots a_n\cdots$ 不能够化成为循环小数发生矛盾.

设 $b_1=2^\alpha 5^\beta$，其中 α，β 都是非负整数，则由 $0<a_1<b_1$，$(a_1, b_1)=1$，(28)式和引理 1 知道 $0.a_1a_2a_3\cdots a_n\cdots$ 能够化成为有限小数，这和假设 $0.a_1a_2a_3\cdots a_n\cdots$ 不能够化成为有限小数发生矛盾.

设 $b_1=2^\alpha 5^\beta b_2$，其中 α，β 都是非负整数，但不同时都是 0，又 $b_2>1$，$(b_2, 10)=1$. 由 $0<a_1<b_1$，$(a_1, b_1)=1$，(28)式和引理 5 我们知道 $0.a_1a_2\cdots a_n\cdots$ 能够化成为循环小数，这和假设 $0.a_1a_2\cdots a_n\cdots$ 不能够化成为循环小数发生矛盾，故本引理得证.

§3. 正数的开 n 次方

在本节中我们假定 n 是一个 $\geqslant 2$ 的整数，而 a 是一个正数. 令 x 是满足方程式

$$x^n=a$$

的一个正数解，那末我们称 x 是 a 的 n 次方根，并把 x 写成为 $\sqrt[n]{a}$（当 $n=2$ 时，令 $\sqrt[2]{a}=\sqrt{a}$）.

有些正整数 a 使得 $\sqrt[n]{a}$ 等于一个正整数. 例如 $\sqrt{361}=19$，$\sqrt[3]{343}=7$，$\sqrt[5]{243}=3$，$\sqrt[8]{6561}=3$. 有些正整数 a 使得 $\sqrt[n]{a}=b+c$，其中 b 是一个正整数而 $0<c<1$. 例如

$$\sqrt{19}=4.3588989\cdots,\quad \sqrt[4]{18941}=11.7314238\cdots.$$

引理 7 设 p 是一个素数，m 是一个正整数且 $m=n\alpha+\beta$，其中 α 是一个非负整数而 β 是一个不大于 $n-1$ 的非负整

数．令 $a=p^m$，当 $\beta=0$ 时，$\sqrt[n]{a}$ 是一个整数．当 $1\leqslant\beta\leqslant n-1$ 时，$\sqrt[n]{a}$ 不能够表示成为分数．

证 （一）当 $\beta=0$时．这时有 $m=n\alpha$ 和 $a=p^{n\alpha}$，故得到 $\sqrt[n]{a}=p^{\alpha}$ 是一个整数．

（二）当 $\alpha=0$ 而 $1\leqslant\beta\leqslant n-1$ 时．这时有 $m=\beta$ 和 $a=p^{\beta}$．如果存在二个正整数b，c 使得 $\sqrt[n]{a}=\frac{b}{c}$ 成立，设 $(b,c)=d$，则有 $b=b_1d$，$c=c_1d$ 而 $(b_1,c_1)=1$．由 $\sqrt[n]{a}=\frac{b}{c}$ 我们有$\sqrt[n]{p^{\beta}}=\sqrt[n]{a}=\frac{b}{c}=\frac{b_1}{c_1}$，$p^{\beta}=\left(\frac{b_1}{c_1}\right)^n$，因而我们有

$$b_1^n=p^{\beta}c_1^n. \tag{29}$$

由 $(b_1,c_1)=1$ 和 (29) 式我们有 $p|b_1$．设 $b_1=p^lb_2$，其中 l 是一个正整数，$(b_2,p)=1$．由 (29) 我们有

$$c_1^n=p^{nl-\beta}b_2^n. \tag{30}$$

由于 $1\leqslant\beta\leqslant n-1$，$l\geqslant1$ 和 (30) 式，所以有 $p|c_1$．由于 $p|b_1$，$p|c_1$，这和 $(b_1,c_1)=1$ 发生矛盾，故不存在二个正整数 b，c 使得 $\sqrt[n]{a}=\frac{b}{c}$ 成立．

（三）当 α 是一个正整数而 $1\leqslant\beta\leqslant n-1$ 时．这时如果存在二个正整数 b，c 使得 $\sqrt[n]{a}=\frac{b}{c}$，则由 $\frac{b}{c}=\sqrt[n]{a}=\sqrt[n]{p^{n\alpha+\beta}}=p^{\alpha}\sqrt[n]{p^{\beta}}$ 得到，$\sqrt[n]{p^{\beta}}=\frac{b}{cp^{\alpha}}$ 是能够表示成为分数的，这和（二）中所证明 $\sqrt[n]{p^{\beta}}$ 不能够表示成为分数发生矛盾．故本引理得证．

引理 8 设 p 是一个素数，m 是一个正整数，$m=n\alpha+\beta$，其中 α 是一个非负整数而 β 是一个不大于 $n-1$ 的非负整数．令 $a=p^m$，当 $\beta=0$ 时，则 $\sqrt[n]{a}$ 是一个正整数．当 $1\leqslant\beta\leqslant$

$n-1$ 时，则有 $\sqrt[n]{a}=b+c$，其中 b 是一个正整数而 c 是一个无限小数但不是循环小数.

证 设 $1\leqslant\beta\leqslant n-1$，而 c 是一个有限小数，则 c 能够化成为分数，即 $c=\frac{a_1}{b_1}$，其中 a_1，b_1 都是正整数. 当 $1\leqslant\beta\leqslant n-1$ 时，则有 $\sqrt[n]{a}=b+c=\frac{b_1b+a_1}{b_1}$. 即这时 $\sqrt[n]{a}$ 能够表示成为分数，这和引理 7 发生矛盾，故 c 不能是一个有限小数而是一个无限小数. 设 c 是一个循环小数，则 c 也能够化成为分数. 因而当 $1\leqslant\beta\leqslant n-1$ 时，$\sqrt[n]{a}$ 也能够表示成为分数，这和引理 7 发生矛盾. 故 c 不是循环小数，本引理得证.

引理 9 设 a 是一个正整数，当 $\sqrt[n]{a}=b+c$ 中 b 是一个正整数而 $0<c<1$ 时，则 $\sqrt[n]{a}$ 不能够表示成为分数，并且这时 c 是一个无限小数但不是循环小数.

证明见习题.

设 a 和 t 都是正整数而 $b=0.a_1\cdots a_t$. 其中 $a_i(i=1,2,\cdots,t)$ 都是不大于 9 的非负整数，但是在 $a_1,\cdots,a_t$ 中至少存在一个正整数. 令 c 是一个正整数，它使得 $(c-1)n<t\leqslant cn$ 成立，则我们有

$$\sqrt[n]{a+b}=\frac{\sqrt[n]{10^{nc}a+10^{nc-1}a_1+\cdots+10^{nc-t}}}{10^c}$$

$$=\frac{A+B}{10^c}. \tag{31}$$

其中 A 是一个正整数而 $0\leqslant B<1$. 当 $0<B<1$ 时，则由引理 9 知道 B 是一个无限小数但不是循环小数.

例 7 求 3.652264 的立方根.

解 由 (31) 式我们有

$$\sqrt[3]{3.652264}=\frac{\sqrt[3]{3652264}}{10^2}. \qquad (32)$$

由于 $3652264 = 2^3 \times 7^3 \times 11^3$，故由 (32) 式得到

$$\sqrt[3]{3.652264}=\frac{2\times 7\times 11}{100}=1.54.$$

例 8 求 7.93 的平方根.

解 由 (31) 式我们有

$$\sqrt{7.93}=\frac{\sqrt{793}}{10}. \qquad (33)$$

由于 $793 = 61 \times 13$，其中 61 和 13 都是素数，由表 1 我们有

150 以下的素数的平方根表

（表一）

p	$\sqrt{p}$	p	$\sqrt{p}$
2	1.41421356…	67	8.18535277…
3	1.73205080…	71	8.42614977…
5	2.23606797…	73	8.54400374…
7	2.64575131…	79	8.88819441…
11	3.3166247…	83	9.11043357…
13	3.60555127…	89	9.43398113…
17	4.12310562…	97	9.84885780…
19	4.35889894…	101	10.0498756…
23	4.79583152…	103	10.1488915…
29	5.38516480…	107	10.3440804…
31	5.56776436…	109	10.4403065…
37	6.0827625…	113	10.6301458…
41	6.40312423…	127	11.2694276…
43	6.55743852…	131	11.4455231…
47	6.85565460…	137	11.7046999…
53	7.28010988…	139	11.7898261…
59	7.68114574…	149	12.2065556…
61	7.81024967…		

60 以下的素数的立方根和五次方根表

（表二）

p	$\sqrt[3]{p}$	p	$\sqrt[5]{p}$
2	1.2599210…	2	1.1486983…
3	1.4422495…	3	1.2457309…
5	1.7099759…	5	1.37972966…
7	1.9129311…	7	1.4757731…
11	2.22398009…	11	1.6153942…
13	2.35133468…	13	1.6702776…
17	2.57128159…	17	1.7623403…
19	2.66840164…	19	1.8019831…
23	2.8438669…	23	1.8721712…
29	3.07231682…	29	1.9610090…
31	3.14138065…	31	1.9873407…
37	3.3322218…	37	2.0589241…
41	3.44821724…	41	2.10163247…
43	3.50339806…	43	2.1217474…
47	3.6088260…	47	2.1598300…
53	3.7562857…	53	2.2123568…
59	3.8929964…	59	2.2603224…

$$\sqrt{61}=7.81024967\cdots,\quad \sqrt{13}=3.60555127\cdots. \qquad (34)$$

由（33）和（34）式我们有

$$\sqrt{7.93}=\frac{(7.81024967\cdots)\times(3.60555127\cdots)}{10}$$

$$=2.81602556\cdots.$$

例 9 求 2.571353 的平方根.

解 由（31）式我们有

$$\sqrt{2.571353}=\frac{\sqrt{2571353}}{10^3}. \qquad (35)$$

由于 $2571353=137^3$，其中 137 是一个素数，由表 1 我们有

$$\sqrt{137}=11.7046999\cdots. \tag{36}$$

由(35)和(36)式我们有

$$\sqrt{2.571353}=\frac{137\times(11.7046999\cdots)}{10^3}=1.60354388\cdots.$$

例 10 求 194400 的十次方根.

解 由于 $194400=2^6\times3^5\times5^2$，所以我们有

$$\sqrt[10]{194400}=\sqrt{2}\times\sqrt{3}\times\sqrt[5]{5}. \tag{37}$$

由表 1 我们有

$$\sqrt{2}=1.41421356\cdots,\quad \sqrt{3}=1.73205080\cdots. \tag{38}$$

由表 2 我们有

$$\sqrt[5]{5}=1.37972966\cdots. \tag{39}$$

由(37)到(39)式我们有

$$\sqrt[10]{194400}=(1.41421356\cdots)\times(1.7320508\cdots)\times(1.37972966\cdots)=3.3796336\cdots.$$

例 11 求 297.756989 的六次方根.

解 由(31)式我们有

$$\sqrt[6]{297.756989}=\frac{\sqrt[6]{297756989}}{10}. \tag{40}$$

由于 $297756989=(17)^2\times(101)^3$，所以有

$$\sqrt[6]{297756989}=\sqrt[3]{17}\times\sqrt{101}.$$

由表 1 我们有$\sqrt{101}=10.0498756\cdots$，由表 2 我们有$\sqrt[3]{17}=2.57128159\cdots$，故得到

$$\sqrt[6]{297756989}=(10.0498756\cdots)(2.57128159\cdots)=25.841060\cdots.$$

故由(40)式得到

$$\sqrt[6]{297.756989} = 2.5841060\cdots.$$

§4. 实数、有理数和无理数

定义 3 一个数 a 能够表示成为 $b+c$（即 $a=b+c$），其中 b 是一个整数而 c 是下面三种情形

（1） 0

（2） 有限小数

（3） 无限小数

中的任意一种，那末我们把 a 叫作一个实数.

定义 4 一个数 a 能够表示成为 $\frac{b}{c}$（即 $a=\frac{b}{c}$），其中 b 是一个整数而 c 是一个正整数，那末我们把 a 叫作一个有理数.

正整数，负整数，0，真分数，假分数，带分数，纯循环小数，混循环小数都是有理数.

定义 5 一个数 a 是一个实数但不是一个有理数，那末我们把数 a 叫作一个无理数.

例如当 a，n 都是大于 1 的正整数，b 是一个正整数而 $0<c<1$，如果有 $\sqrt[n]{a}=b+c$，那末 $\sqrt[n]{a}$ 就是一个无理数.

定义 6 把半径为 $\frac{1}{2}$ 的圆的圆周的长度记作 π.

我们可以使用较高深的数论方法来证明 π 是一个无理数，经过计算我们有

$$\pi = 3.141592654\cdots. \tag{41}$$

我国古代数学家何承天（370—447）发明用 $\frac{22}{7}$ 表示 π 的近似值，祖冲之（429—500）发明用 $\frac{355}{113}$ 作为 π 的近似值，而西

欧最早发现这一事实的时间比他还晚一千多年．事实上，$\frac{355}{113}=3.1415929\cdots$与$\pi$的真值的前六位小数是符合的，由此可见祖氏在数学上的成就是非常突出的．他是历史上第一流数学家，他的成就是我们祖国的光荣．他的非常突出的成就主要是由于他自己的刻苦学习和劳动得来的．他曾说过他学习算学是"……搜练古今，博采沈奥，唐篇夏典，莫不揆量，周正汉朔，咸加该验……"．通过祖冲之的成就和事迹，再一次证明了中国人民是勤劳、勇敢而又有高度智慧的．

定义7 设k是一个正整数，我们用$k!$来表示$1\times2\times\cdots\times k$，即

$$k!=1\times2\times\cdots\times k.$$

例如 $1!=1$，$2!=1\times2=2$，$3!=1\times2\times3=6$，$4!=1\times2\times3\times4=24$，$5!=1\times2\times3\times4\times5=120$，$6!=1\times2\times3\times4\times5\times6=720$，$7!=5040$，$8!=40320$．

设 $a_1, a_2, \cdots, a_n$ 都是实数，为了简单起见我们把 $a_1+a_2+\cdots+a_n$ 的和记作 $\sum\limits_{k=1}^{n} a_k$．即

$$\sum_{k=1}^{n} a_k=a_1+a_2+\cdots+a_n.$$

例12 求 $\sum\limits_{k=1}^{8}\frac{1}{k!}$ 等于多少．

解
$$\begin{aligned}\sum_{k=1}^{8}\frac{1}{k!}&=1+\frac{1}{2!}+\frac{1}{3!}+\frac{1}{4!}+\frac{1}{5!}+\frac{1}{6!}+\frac{1}{7!}+\frac{1}{8!}\\&=1+\frac{1}{2}+\frac{1}{6}+\frac{1}{24}+\frac{1}{120}+\frac{1}{720}+\frac{1}{5040}\\&\quad+\frac{1}{40320}=1.71827877\cdots.\end{aligned}$$

例 13 求 $\sum_{k=1}^{15}\frac{1}{k^2}$ 等于多少.

解
$$\sum_{k=1}^{15}\frac{1}{k^2}=1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\frac{1}{5^2}+\frac{1}{6^2}+\frac{1}{7^2}+\frac{1}{8^2}+\frac{1}{9^2}+\frac{1}{10^2}+\frac{1}{11^2}+\frac{1}{12^2}+\frac{1}{13^2}+\frac{1}{14^2}+\frac{1}{15^2}$$
$$=1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\frac{1}{25}+\frac{1}{36}+\frac{1}{49}+\frac{1}{64}+\frac{1}{81}+\frac{1}{100}+\frac{1}{121}+\frac{1}{144}+\frac{1}{169}+\frac{1}{196}+\frac{1}{225}$$
$$=1.58044028\cdots.$$

例 14 求 $\sum_{k=1}^{11}\frac{1}{k!}$ 等于多少.

解
$$\sum_{k=1}^{11}\frac{1}{k!}=\sum_{k=1}^{8}\frac{1}{k!}+\frac{1}{9!}+\frac{1}{10!}+\frac{1}{11!}$$
$$=1.71827877\cdots+\frac{1}{362880}+\frac{1}{3628800}+\frac{1}{39916800}=1.71828182\cdots.$$

定义 8 我们把无限大记作 ∞.

使用较高深的数论方法我们可以证明 $\sum_{k=1}^{\infty}\frac{1}{k^2}=\frac{\pi^2}{6}$. 令 $0!=1$ 及

$$e=\sum_{k=0}^{\infty}\frac{1}{k!}=2.718281828\cdots,$$

使用较高深的数论方法我们可以证明 e 是一个无理数. 令 a 是任一个大于 1 的整数而 $\xi = 1 + \frac{1}{a^{2!}} + \frac{1}{a^{3!}} + \frac{1}{a^{4!}} + \cdots = \sum_{n=0}^{\infty} \frac{1}{a^{n!}}$，我们可以使用较高深的数论方法来证明 ξ 是一个无理数.

设 a，b 都是有理数，则有 $a = \frac{c_1}{d_1}$，$b = \frac{c_2}{d_2}$，其中 c_1，c_2 都是整数而 d_1，d_2 都是正整数. 因而我们有

$$ab = \frac{c_1c_2}{d_1d_2},$$

其中 c_1c_2 是整数，d_1d_2 是一个正整数，所以 ab 也是一个有理数，即二个有理数相乘是一个有理数. 设 A 是一个无理数而 a 是一个有理数，其中 $a = \frac{b}{c}$，又 $b \neq 0$ 是一个整数，而 c 是一个正整数，则 $a \times A$ 是一个无理数. 因为假设 $a \times A = a_1$，而 a_1 是一个有理数，由 $a = \frac{b}{c}$ 而 $b \neq 0$ 和 $a \times A = a_1$，所以有 $a_1 \neq 0$. 设 $a_1 = \frac{b_1}{c_1}$，其中 b_1 是一个整数而 c_1 是一个正整数. 由 $a_1 \neq 0$ 故有 $b_1 \neq 0$. 由 $a \times A = a_1$ 得到 $A = \frac{a_1}{a} = \frac{b_1c}{bc_1}$，则 A 是一个有理数，这和假设 A 是一个无理数发生矛盾. 所以不等于 0 的有理数乘无理数是一个无理数.

习　题

1. 把下列分数化为小数:

(i) $\frac{371}{6250}$，(ii) $\frac{190}{37}$，(iii) $\frac{13}{28}$，

(iv) $\frac{a}{875}$, $a = 4$, 29, 139, 361.

2. 把下列小数化为分数:

(i) 0.868, (ii) $0.8\dot{3}65\dot{4}$, (iii) $0.37\dot{6}8935\dot{4}$.

3.(引理 9) 设 a 是一个正整数,当 $\sqrt[n]{a} = b + c$, 其中 b 是一个正整数而 $0 < c < 1$ 时,则$\sqrt[n]{a}$不能够表示成为分数,这时 c 是一个无限小数但不是循环小数.

4. 证明: 整系数方程

$$x^n + a_1x^{n-1} + \cdots + a_n = 0, \quad n \geqslant 1$$

的实数根如果不是整数就一定是无理数.

5. 证明: $\log_{10} 2$ 是无理数.

6. 若正整数 M 和 N 不能表示成同底数的正整数幂时(底数也是正整数), $\log_M N$ 一定是无理数.

7. 试证: e 是无理数.

8. 证明:

$$J = 1 - \frac{1}{2^2} + \frac{1}{2^2 \cdot 4^2} - \frac{1}{2^2 \cdot 4^2 \cdot 6^2} + \cdots$$

是无理数.

9. 对于任意实数 α, 我们定义 $[\alpha]$ 为不大于 α 的最大整数. 试证: 对于正整数 a 和 b, 不大于 a 而为 b 的倍数的正整数共有$\left[\frac{a}{b}\right]$个.

10. 在 $n!$ 的标准分解式中,素数 p 的方次数为

$$S = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots = \sum_{r=1}^{\infty} \left[\frac{n}{p^r}\right].$$

11. 设若 $3^k | 1000!$ 而 $3^{k+1} \nmid 1000!$, 求 k.

12. 设 $C_m^n = \frac{m!}{n!(m-n)!}$, m, n 是正整数且 $m > n$, 试

证:

(i) $C_m^n = C_m^{m-n}$;

(ii) C_m^n 是正整数;

(iii) k 个连续正整数的乘积能被 $k!$ 整除;

(iv) 设 p 是素数, $k < p$, 则 $p \mid C_p^k$.

13. 试证:

(i) Wilson 定理: 设 p 是素数,则有

$$(p-1)! \equiv -1 \pmod p.$$

(ii) 若 $(p-1)! \equiv -1 \pmod p$,则 p 是素数.

14. 当 n 和 $n+2$ 都是素数时,称 n 和 $n+2$ 为一对孪生素数. 试证: n 和 $n+2$ 是孪生素数的充分必要条件是

$$4[(n-1)!+1]+n \equiv 0 \ [\bmod n(n+2)], \quad n > 1.$$

15. 设 $a^{m-1} \equiv 1 \pmod m$, 而对于 $m-1$ 的任意约数 n, 当 $0 < n < m-1$ 时, $a^n \not\equiv 1 \pmod m$,则 m 是素数.

16. 设 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, $d(n)$ 表示 n 的所有约数的个数, $\sigma(n)$ 表示 n 的所有约数的和. 试证:

(i) $d(n) = (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_n+1)$.

(ii) $\sigma(n) = \left(\dfrac{p_1^{\alpha_1+1}-1}{p_1-1}\right)\left(\dfrac{p_2^{\alpha_2+1}-1}{p_2-1}\right)\cdots\left(\dfrac{p_n^{\alpha_n+1}-1}{p_n-1}\right)$.

17. 设 n 是正整数, $n \geqslant 2$. 试证: n 是素数的充分必要条件是

$$\varphi(n) \mid (n-1) \text{ 且 } (n+1) \mid \sigma(n).$$

第七章　连分数和数论函数

§1. 连分数的基本概念

设 b 是一个 $\geqslant 1$ 的正数，利用 $(\sqrt{b^2+1}+b)(\sqrt{b^2+1}-b)=(\sqrt{b^2+1})^2-b^2=1$，得到

$$\sqrt{b^2+1}-b=\frac{1}{\sqrt{b^2+1}+b}. \tag{1}$$

连续利用 (1) 式我们有

$$\sqrt{b^2+1}=b+\sqrt{b^2+1}-b=b+\frac{1}{\sqrt{b^2+1}+b}$$

$$=b+\frac{1}{2b+\sqrt{b^2+1}-b}$$

$$=b+\cfrac{1}{2b+\cfrac{1}{\sqrt{b^2+1}+b}}$$

$$=b+\cfrac{1}{2b+\cfrac{1}{2b+\sqrt{b^2+1}-b}}$$

$$=b+\cfrac{1}{2b+\cfrac{1}{2b+\cfrac{1}{\sqrt{b^2+1}+b}}}$$

$$=b+\cfrac{1}{2b+\cfrac{1}{2b+\cfrac{1}{2b+\sqrt{b^2+1}-b}}}$$

$$=\cdots=b+\cfrac{1}{2b+\cfrac{1}{2b+\cfrac{}{\ddots+\cfrac{1}{2b}+\cdots}}}. \quad (2)$$

以后我们将证明下面的二式都能够成立:

$$b+\cfrac{1}{2b+\cfrac{1}{2b}}\leqslant\sqrt{b^2+1}\leqslant b+\cfrac{1}{2b+\cfrac{1}{2b+\cfrac{1}{2b}}}, \quad (3)$$

$$b+\cfrac{1}{2b+\cfrac{1}{2b+\cfrac{1}{2b+\cfrac{1}{2b}}}}\leqslant\sqrt{b^2+1}. \quad (4)$$

由于 $2b+\frac{1}{2b}=\frac{4b^2+1}{2b}$，所以我们有

$$\cfrac{1}{2b+\cfrac{1}{2b}}=\frac{2b}{4b^2+1}. \quad (5)$$

由(5)式得到 $2b+\cfrac{1}{2b+\cfrac{1}{2b}}=\frac{8b^3+4b}{4b^2+1}$，所以我们有

$$\cfrac{1}{2b+\cfrac{1}{2b+\cfrac{1}{2b}}}=\frac{4b^2+1}{8b^3+4b}. \quad (6)$$

由(6)式得到

$$2b+\cfrac{1}{2b+\cfrac{1}{2b+\cfrac{1}{2b}}}=2b+\frac{4b^2+1}{8b^3+4b}$$

$$=\frac{16b^4+12b^2+1}{8b^3+4b},$$

因而我们有

$$\cfrac{1}{2b+\cfrac{1}{2b+\cfrac{1}{2b+\cfrac{1}{2b}}}}=\frac{8b^3+4b}{16b^4+12b^2+1}. \tag{7}$$

由 (5) 式我们有

$$b+\cfrac{1}{2b+\cfrac{1}{2b}}=\frac{4b^3+3b}{4b^2+1}. \tag{8}$$

由 (6) 式我们有

$$b+\cfrac{1}{2b+\cfrac{1}{2b+\cfrac{1}{2b}}}=\frac{8b^4+8b^2+1}{8b^3+4b}. \tag{9}$$

由 (3), (8) 和 (9) 式我们有

$$\frac{4b^3+3b}{4b^2+1}\leqslant\sqrt{b^2+1}\leqslant\frac{8b^4+8b^2+1}{8b^3+4b}. \tag{10}$$

由 (4) 和 (7) 式我们有

$$\frac{16b^5+20b^3+5b}{16b^4+12b^2+1}\leqslant\sqrt{b^2+1}\leqslant\frac{8b^4+8b^2+1}{8b^3+4b}. \tag{11}$$

例 1 求证

$\sqrt{101}=10.0498756211\cdots$, $\sqrt{65}=8.0622577\cdots$.

证 在(11)式中取 $b=10$，则得到

$$10.0498756211 \leqslant \frac{1620050}{161201} \leqslant \sqrt{101}$$

$$\leqslant \frac{80801}{8040} \leqslant 10.0498756219.$$

故得到 $\sqrt{101}=10.0498756211\cdots$. 在(11)式中取 $b=8$，则我们有

$$8.062257747 \leqslant \frac{534568}{66305} \leqslant \sqrt{65}$$

$$\leqslant \frac{33281}{4128} \leqslant 8.062257753.$$

故得到

$$\sqrt{65}=8.0622577\cdots.$$

设 b 是一个 $\geqslant 2$ 的正数，利用 $(\sqrt{b^2-1}-b+1)\times(\sqrt{b^2-1}+b-1)=b^2-1-(b-1)^2=2(b-1)$，得到

$$\sqrt{b^2-1}-b+1=\frac{2(b-1)}{\sqrt{b^2-1}+b-1}. \qquad (12)$$

继续利用(12)式我们有

$$\begin{aligned}\sqrt{b^2-1}&=b-1+\sqrt{b^2-1}-b+1\\&=b-1+\frac{2(b-1)}{\sqrt{b^2-1}+b-1}\\&=b-1+\cfrac{1}{\cfrac{2(b-1)+\sqrt{b^2-1}-b+1}{2(b-1)}}\\&=b-1+\cfrac{1}{1+\cfrac{1}{\sqrt{b^2-1}+b-1}}\end{aligned}$$

$$=b-1+\cfrac{1}{1+\cfrac{1}{2(b-1)+\sqrt{b^2-1}-b+1}}$$

$$=b-1+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{2(b-1)}{\sqrt{b^2-1}+b-1}}}$$

$$=b-1+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{2(b-1)}{2(b-1)+\sqrt{b^2-1}-b+1}}}$$

$$=b-1+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{\sqrt{b^2-1}+b-1}}}}$$

$$=\cdots=b-1$$

$$+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cdots}}}}}}. \quad (13)$$

由于$1+\frac{1}{2(b-1)}=\frac{2b-1}{2(b-1)}$，得到$2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)}}$

$$=2(b-1)+\frac{2(b-1)}{2b-1}=\frac{4b^2-4b}{2b-1},$$

因而 $1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)}}}=1+\dfrac{2b-1}{4b^2-4b}$

$$=\frac{4b^2-2b-1}{4b^2-4b}.$$

我们有 $2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)}}}}$

$$=2(b-1)+\frac{4b^2-4b}{4b^2-2b-1}=\frac{8b^3-8b^2-2b+2}{4b^2-2b-1},$$

得到 $1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)}}}}}$

$$=1+\frac{4b^2-2b-1}{8b^3-8b^2-2b+2}=\frac{8b^3-4b^2-4b+1}{8b^3-8b^2-2b+2}. \quad (14)$$

由于 $2(b-1)+1=2b-1$， $1+\dfrac{1}{2b-1}=\dfrac{2b}{2b-1}$,

$$\cfrac{1}{1+\cfrac{1}{2b-1}}=\frac{2b-1}{2b},$$

$$2(b-1)+\cfrac{1}{1+\cfrac{1}{2b-1}}=2(b-1)+\frac{2b-1}{2b}=\frac{4b^2-2b-1}{2b},$$

$$1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2b-1}}}=1+\frac{2b}{4b^2-2b-1}$$

$$=\frac{4b^2-1}{4b^2-2b-1},\ 2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2b-1}}}}$$

$$=2(b-1)+\frac{4b^2-2b-1}{4b^2-1}=\frac{8b^3-4b^2-4b+1}{4b^2-1},$$

所以我们有

$$1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2b-1}}}}}$$

$$=1+\frac{4b^2-1}{8b^3-4b^2-4b+1}=\frac{8b^3-4b}{8b^3-4b^2-4b+1}. \tag{15}$$

以后我们将由（13）式证明下面的式子能够成立

$$b-1+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)}}}}}}$$

$$\leqslant\sqrt{b^2-1}\leqslant b-1$$

$$+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2b-1}}}}}}. \tag{16}$$

由(14)到(16)式我们有

$$b-1+\frac{8b^3-8b^2-2b+2}{8b^3-4b^2-4b+1}\leqslant\sqrt{b^2-1}\leqslant b-1$$
$$+\frac{8b^3-4b^2-4b+1}{8b^3-4b}. \tag{17}$$

例 2 求证$\sqrt{11}=3.3166247\cdots$.

证 在(17)式中取 $b=10$，则得到 $9.949874355\leqslant 9+\frac{7182}{7561}\leqslant\sqrt{99}\leqslant 9+\frac{7561}{7960}\leqslant 9.949874372$，所以$\sqrt{11}=\frac{\sqrt{99}}{3}=3.3166247\cdots$.

§2. 数学归纳法

数学归纳法是在数论中被广泛地应用的方法. 数学归纳法的用途是它可以推断某些在一系列的特殊情形已经成立了的数学命题在一般的情形下是不是也真确. 它的原则是这样的:

假如有一个数学命题符合下面二个条件: (1) 这个命题对 $n=1$ 是真确的; (2) 假设这个命题对任一个正整数 $n=k-1$ 是真确的,那末我们就可以推出它对于 $n=k$ 也真确; 则我们说这个命题对于所有的正整数 n 都是真确的.

如果我们说数学归纳法的原则不是真确的, 那就是说这个命题并非对于所有的正整数 n 都是真确的, 那末我们一定可以找到一个最小的使命题不真确的正整数 m. 由于已知这个命题对 $n=1$ 是真确的,所以 m 一定大于1. 由于 m 是一个大于1的正整数,所以 $m-1$ 也是一个正整数. 但 m 是使命题不真确的最小的正整数,由于 $m-1$ 小于 m, 所以命题对 $n=m-1$ 一定真确. 这样就得出,对于正整数 $m-1$ 命题是真确的,而对于紧接着的正整数 m, 命题不真确. 这和数学归纳法原则中的条件 (2) 相冲突.

下面举一些用数学归纳法证明问题的例子.

例 3 证明 n^3+5n 是6的倍数(这里 n 是一个正整数).

证 这里的数学命题就是指 n^3+5n 是6的倍数.

(1) 当 $n=1$ 时有 $n^3+5n=6$, 因而当 $n=1$ 时数学命题成立.

(2) 设 k 是一个 $\geqslant 2$ 的整数. 令这个数学命题对 $n=k-1$ 成立,即假定

$$(k-1)^3+5(k-1)=6m$$

成立，其中 m 是一个整数.由此来推出 k^3+5k 是6的倍数.事实上，由归纳法假设

$$\begin{aligned}k^3+5k&=(k-1+1)^3+5(k-1)+5\\&=(k-1)^3+3(k-1)^2+3(k-1)\\&\quad+1+5(k-1)+5\\&=(k-1)^3+5(k-1)+3(k-1)k+6\\&=6\left(m+1+\frac{k(k-1)}{2}\right).\end{aligned}$$

由于 k 是一个整数，所以 $\frac{k(k-1)}{2}$ 也是一个整数，因而 $m+1+\frac{k(k-1)}{2}$ 是一个整数．由此说明 k^3+5k 确实是6的倍数．因而 n^3+5n 是6的倍数对所有的正整数 n 都成立．

例4 设 n 是一个正整数，$x_1,\cdots,x_n,y_1,\cdots,y_n$ 都是实数，则

$$(x_1y_1+\cdots+x_ny_n)^2\leqslant(x_1^2+\cdots+x_n^2)(y_1^2+\cdots+y_n^2)\tag{18}$$

成立．

证 这里的数学命题是(18)式是真确的．

(1) 当 $n=1$ 时我们有 $x_1^2y_1^2\geqslant(x_1y_1)^2$，故(18)式是成立的．

(2) 设 k 是一个 $\geqslant 2$ 的整数．令这个数学命题对 $n=k-1$ 成立．即假定

$$(x_1y_1+\cdots+x_{k-1}y_{k-1})^2\leqslant(x_1^2+\cdots+x_{k-1}^2)\times(y_1^2+\cdots+y_{k-1}^2)\tag{19}$$

成立．由此来推出 $(x_1y_1+\cdots+x_ky_k)^2\leqslant(x_1^2+\cdots+x_k^2)\times(y_1^2+\cdots+y_k^2)$ 成立．由(19)式我们有

$$(x_1y_1+\cdots+x_{k-1}y_{k-1}+x_ky_k)^2=(x_1y_1+\cdots+x_{k-1}y_{k-1})^2$$
$$+x_k^2y_k^2+2x_ky_k(x_1y_1+\cdots+x_{k-1}y_{k-1})\leqslant(x_1^2+\cdots+x_{k-1}^2)$$
$$\times(y_1^2+\cdots+y_{k-1}^2)+x_k^2y_k^2+2x_ky_k(x_1y_1+\cdots+x_{k-1}y_{k-1}).\tag{20}$$

由于 x_i，y_i（其中 $i=1, 2,\cdots, k$）都是实数，所以我们有 $x_k^2y_i^2+x_i^2y_k^2-2x_ky_kx_iy_i=(x_ky_i-x_iy_k)^2\geqslant 0$，即 $2x_ky_kx_iy_i\leqslant x_k^2y_i^2+x_i^2y_k^2$．故得到

$$x_k^2y_k^2+2x_ky_k(x_1y_1+\cdots+x_{k-1}y_{k-1})$$
$$\leqslant x_k^2(y_1^2+\cdots+y_k^2)+y_k^2(x_1^2+\cdots+x_{k-1}^2).\tag{21}$$

由 (20) 和 (21) 式我们有

$$(x_1y_1+\cdots+x_ky_k)^2\leqslant(x_1^2+\cdots+x_k^2)(y_1^2+\cdots+y_k^2),$$

即 (18) 式对于所有的正整数 n 都成立．

§3. 连分数的基本性质

设 a_1 是实数，而 $a_2,\cdots, a_n$ 都是 $\geqslant 1$ 的实数，我们把分数

$$a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\ddots+\cfrac{1}{a_n}}}\tag{22}$$

叫作有限连分数，不过 (22) 的写法很占篇幅，故常用符号

$$a_1+\frac{1}{a_2}+\frac{1}{a_3}+\frac{1}{a_4}+\cdots+\frac{1}{a_n}\tag{23}$$

或
$$[a_1, a_2,\cdots, a_n]\tag{24}$$

来表示有限连分数 (22)．

注意：此处 (24) 表示连分数 (22)，而不是表示最小公倍数．

定义 1 当 $1\leqslant k\leqslant n$ 是一个整数时，我们把 $[a_1, a_2,\cdots,$

$a_k] = \frac{p_k}{q_k}$ 叫作(22)的第 k 个渐近分数.

由定义 1 可以知道 $\frac{p_k}{q_k}$ 是和 $a_1, a_2, \cdots, a_k$ 有关的，但是和 $a_{k+1}, \cdots, a_n$ 没有关系. 由于

$$[a_1] = a_1 = \frac{a_1}{1},$$

所以有

$$\frac{p_1}{q_1} = \frac{a_1}{1}.$$

由于

$$[a_1, a_2] = a_1 + \frac{1}{a_2} = \frac{a_1a_2 + 1}{a_2},$$

所以有

$$\frac{p_2}{q_2} = \frac{a_1a_2 + 1}{a_2}.$$

由于

$$[a_1, a_2, a_3] = a_1 + \frac{1}{a_2 + \frac{1}{a_3}} = a_1 + \frac{1}{\frac{a_2a_3 + 1}{a_3}}$$

$$= a_1 + \frac{a_3}{a_2a_3 + 1} = \frac{a_3(a_1a_2 + 1) + a_1}{a_2a_3 + 1},$$

所以有

$$\frac{p_3}{q_3} = \frac{a_3(a_1a_2 + 1) + a_1}{a_2a_3 + 1}.$$

更一般地我们有下面的结果.

引理 1 设 $n \geqslant 3$ 和连分数 $[a_1, a_2, \cdots, a_n]$ 的渐近分数是 $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \cdots, \frac{p_n}{q_n}$，则在这些渐近分数之间，下面的关系式成立

$$p_1 = a_1,\ q_1 = 1,\ p_2 = a_1a_2 + 1,\ q_2 = a_2.$$

而当 $3 \leqslant k \leqslant n$ 时，则有

$$p_k = a_k p_{k-1} + p_{k-2},\ q_k = a_k q_{k-1} + q_{k-2}. \tag{25}$$

证 由于

$$\frac{p_1}{q_1} = \frac{a_1}{1},$$

所以有

$$p_1 = a_1,\ q_1 = 1.$$

由于

$$\frac{p_2}{q_2} = \frac{a_1 a_2 + 1}{a_2},$$

所以有

$$p_2 = a_1 a_2 + 1,\ q_2 = a_2.$$

由于

$$\frac{p_3}{q_3} = \frac{a_3(a_1 a_2 + 1) + a_1}{a_2 a_3 + 1},$$

所以有

$$p_3 = a_3(a_1 a_2 + 1) + a_1 = a_3 p_2 + a_1,$$

$$q_3 = a_2 a_3 + 1 = a_3 q_2 + q_1. \tag{26}$$

由于在(22)式中设有 $a_2, \cdots, a_n$ 都是 $\geqslant 1$ 的实数，所以 q_1，q_2，q_3 都是 $\geqslant 1$ 的实数．由(26)式知道，(25)式当 $k = 3$ 时是成立的，故引理 1 当 $n = 3$ 时是成立的．现设 $n \geqslant 4$．假定(25)式对小于 k 而 $\geqslant 3$ 的整数都能够成立，则由数学归纳法我们有

$$\frac{p_k}{q_k} = [a_1, a_2, \cdots, a_{k-1}, a_k] = [a_1, a_2, \cdots, a_{k-1} + \frac{1}{a_k}]$$

$$= \frac{\left(a_{k-1} + \frac{1}{a_k}\right) p_{k-2} + p_{k-3}}{\left(a_{k-1} + \frac{1}{a_k}\right) q_{k-2} + q_{k-3}}$$

$$= \frac{(a_k a_{k-1} + 1) p_{k-2} + a_k p_{k-3}}{(a_k a_{k-1} + 1) q_{k-2} + a_k q_{k-3}}$$

$$= \frac{a_k(a_{k-1} p_{k-2} + p_{k-3}) + p_{k-2}}{a_k(a_{k-1} q_{k-2} + q_{k-3}) + q_{k-2}}.$$

故得到

$$p_k = a_k(a_{k-1}p_{k-2} + p_{k-3}) + p_{k-2},$$
$$q_k = a_k(a_{k-1}q_{k-2} + q_{k-3}) + q_{k-2}. \tag{27}$$

由(25)式我们有 $p_{k-1}=a_{k-1}p_{k-2}+p_{k-3}$，$q_{k-1}=a_{k-1}q_{k-2}+q_{k-3}$，故由(27)式得到 $p_k = a_kp_{k-1} + p_{k-2}$，$q_k = a_kq_{k-1} + q_{k-2}$。使用数学归纳法知道当 $3 \leqslant k \leqslant n$ 时，(25)式成立。故引理1得证。

引理 2 如果连分数 $[a_1, a_2, \cdots, a_n]$ 的 n 个渐近分数是 $\frac{p_k}{q_k}$(其中 $k = 1, 2, \cdots, n$)，则当 $k \geqslant 2$ 时我们有

$$p_kq_{k-1} - p_{k-1}q_k = (-1)^k, \tag{28}$$

而当 $k \geqslant 3$ 时我们有

$$p_kq_{k-2} - p_{k-2}q_k = (-1)^{k-1}a_k. \tag{29}$$

证 (i) 由于 $p_2 = a_1a_2 + 1$，$q_1 = 1$，$p_1 = a_1$，$q_2 = a_2$，我们有

$p_2q_1 - p_1q_2 = a_1a_2 + 1 - a_1a_2 = 1$. 所以当 $k = 2$ 时(28)式成立。现设 $k \geqslant 3$，设(28)式当 $k-1$ 时是成立的，即 $p_{k-1}q_{k-2} - p_{k-2}q_{k-1} = (-1)^{k-1}$，则由(25)式我们有

$$\begin{aligned} p_kq_{k-1} - p_{k-1}q_k &= (a_kp_{k-1} + p_{k-2})q_{k-1} - p_{k-1}(a_kq_{k-1} + q_{k-2}) \\ &= p_{k-2}q_{k-1} - p_{k-1}q_{k-2} \\ &= -(p_{k-1}q_{k-2} - p_{k-2}q_{k-1}) \\ &= -(-1)^{k-1} = (-1)^k. \end{aligned}$$

故由数学归纳法知道(28)能够成立。

(ii) 由(25)和(28)式我们有

$$\begin{aligned} p_kq_{k-2} - p_{k-2}q_k &= (a_kp_{k-1} + p_{k-2})q_{k-2} - p_{k-2}(a_kq_{k-1} + q_{k-2}) \\ &= a_k(p_{k-1}q_{k-2} - p_{k-2}q_{k-1}) \\ &= (-1)^{k-1}a_k. \end{aligned}$$

故引理2得证。

§4. 把有理数表成连分数

例 5 把 $\frac{107}{95}$ 表成连分数.

解 我们有

$$\frac{107}{95}=1+\frac{12}{95}=1+\cfrac{1}{\frac{95}{12}}=1+\cfrac{1}{7+\frac{11}{12}}$$

$$=1+\cfrac{1}{7+\cfrac{1}{1+\frac{1}{11}}}=[1,7,1,11].$$

例 6 把 $\frac{225}{43}$ 表成连分数.

解 我们有

$$\frac{225}{43}=5+\frac{10}{43}=5+\cfrac{1}{\frac{43}{10}}=5+\cfrac{1}{4+\frac{3}{10}}=5+\cfrac{1}{4+\cfrac{1}{\frac{10}{3}}}$$

$$=5+\cfrac{1}{4+\cfrac{1}{3+\frac{1}{3}}}=[5,4,3,3].$$

引理 3 每一个有理数都能够表示成为有限连分数.

证 设 $\frac{a}{b}$ 是一个有理数,其中 a 是一个整数而 b 是一个正整数,设 $\frac{a}{b}$ 是一个整数,即 $\frac{a}{b}=c$,其中 c 是一个整数,则我们有 $\frac{a}{b}=[c]$.

设 $\frac{a}{b}$ 不是一个整数，则存在二个整数 q_1 和 r_1，使得 $a = bq_1 + r_1$ 成立，其中 $0 < r_1 < b$，即得

$$\frac{a}{b} = q_1 + \frac{r_1}{b} = q_1 + \frac{1}{\frac{b}{r_1}}. \tag{30}$$

设 $\frac{b}{r_1}$ 是一个正整数，即 $\frac{b}{r_1} = c_1$，其中 c_1 是一个正整数，则由 (30) 式我们有 $\frac{a}{b} = [q_1, c_1]$。设 $\frac{b}{r_1}$ 不是一个正整数，则一定存在二个正整数 q_2 和 r_2，使得 $b = r_1 q_2 + r_2$ 成立，其中 $0 < r_2 < r_1$。即得 $\frac{b}{r_1} = q_2 + \frac{r_2}{r_1}$，故由 (30) 式我们有

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{r_2}{r_1}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_1}{r_2}}}, \tag{31}$$

其中 r_1, r_2 都是正整数而 $0 < r_2 < r_1 < b$。设 $\frac{r_1}{r_2}$ 是一个正整数，即 $\frac{r_1}{r_2} = c_2$，其中 c_2 是一个正整数，则由 (31) 式我们有 $\frac{a}{b} = [q_1, q_2, c_2]$。设 $\frac{r_1}{r_2}$ 不是一个正整数，则一定存在二个正整数 q_3 和 r_3，使得 $r_1 = r_2 q_3 + r_3$ 成立，其中 $0 < r_3 < r_2$。即得 $\frac{r_1}{r_2} = q_3 + \frac{r_3}{r_2}$。故由 (31) 式我们有

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{\frac{r_2}{r_3}}}}. \tag{32}$$

用同样的方法进行下去，由于 b，r_1，r_2，r_3，$\cdots$ 都是正整数和 $b > r_1 > r_2 > r_3 > \cdots$，所以最后一定有一个正整数 r_n，它使得

$$\frac{r_{n-2}}{r_{n-1}} = q_n + \frac{r_n}{r_{n-1}}, \quad \frac{r_n}{r_{n-1}} = q_{n+1}, \quad r_{n-2} > r_{n-1} > r_n$$

成立，其中 q_n，q_{n+1} 都是正整数．故得到

$$\frac{a}{b} = [q_1, q_2, \cdots, q_{n+1}].$$ 引理 3 得证．

§5. 无限连分数

定义 2　如果 a_1 是整数而 $a_2, a_3, \cdots, a_k, \cdots$ 都是 $\geqslant 1$ 的实数，则连分数

$$[a_1, a_2, a_3, \cdots, a_k, \cdots]$$

叫作无限连分数．对于无限连分数，我们仍然规定 $\frac{p_k}{q_k} = [a_1, \cdots, a_k]$（其中 $k = 1, 2, \cdots$）是 $[a_1, a_2, a_3, \cdots, a_k, \cdots]$ 的第 k 个渐近分数．又如当 $k \to \infty$ 时，$\frac{p_k}{q_k}$ 有一个极限，我们就把这一极限叫作连分数的值．

显然引理 1 和引理 2 对无限连分数来说仍然成立．

引理 4　设 $[a_1, a_2, \cdots, a_n \cdots]$ 是一个无限连分数，$\frac{p_k}{q_k}$（$k=1, 2, \cdots$）是它的第 k 个渐近分数，则当 $k \geqslant 2$ 时我们有

$$\frac{p_{2(k-1)}}{q_{2(k-1)}} > \frac{p_{2k}}{q_{2k}}, \quad \frac{p_{2k-1}}{q_{2k-1}} > \frac{p_{2k-3}}{q_{2k-3}}, \quad \frac{p_{2k}}{q_{2k}} > \frac{p_{2k-1}}{q_{2k-1}}.$$

证　由于 $a_2, a_3, \cdots, a_k, \cdots$，都是 $\geqslant 1$ 的实数和引理 1，我们有 $q_1, q_2, \cdots, q_k, \cdots$ 都是 $\geqslant 1$ 的实数．由 (29) 式我们有

$$\frac{p_{2(k-1)}}{q_{2(k-1)}}-\frac{p_{2k}}{q_{2k}}=\frac{-(p_{2k}q_{2(k-1)}-p_{2(k-1)}q_{2k})}{q_{2k}q_{2(k-1)}}$$
$$=\frac{(-1)^{2k}a_{2k}}{q_{2k}q_{2(k-1)}}>0,$$
$$\frac{p_{2k-1}}{q_{2k-1}}-\frac{p_{2k-3}}{q_{2k-3}}=\frac{p_{2k-1}q_{2k-3}-p_{2k-3}q_{2k-1}}{q_{2k-1}q_{2k-3}}$$
$$=\frac{(-1)^{2k-2}a_{2k-1}}{q_{2k-1}q_{2k-3}}>0.$$

故得到

$$\frac{p_{2(k-1)}}{q_{2(k-1)}}>\frac{p_{2k}}{q_{2k}},\qquad \frac{p_{2k-1}}{q_{2k-1}}>\frac{p_{2k-3}}{q_{2k-3}}.$$

由(28)式我们有

$$\frac{p_{2k}}{q_{2k}}-\frac{p_{2k-1}}{q_{2k-1}}=\frac{p_{2k}q_{2k-1}-p_{2k-1}q_{2k}}{q_{2k}q_{2k-1}}=\frac{(-1)^{2k}}{q_{2k}q_{2k-1}}>0,$$

故得到

$$\frac{p_{2k}}{q_{2k}}>\frac{p_{2k-1}}{q_{2k-1}}.$$ 故引理得证.

引理 5 设 $[a_1, a_2, \cdots, a_n, \cdots]$ 是一个无限连分数. 当 $k\to\infty$ 时 $\frac{p_k}{q_k}$ 有一极限,则我们有

$$\frac{p_1}{q_1}<\frac{p_3}{q_3}<\frac{p_5}{q_5}<\frac{p_7}{q_7}<\frac{p_9}{q_9}<\cdots<[a_1, a_2, \cdots, a_n, \cdots]$$
$$<\cdots<\frac{p_{10}}{q_{10}}<\frac{p_8}{q_8}<\frac{p_6}{q_6}<\frac{p_4}{q_4}<\frac{p_2}{q_2}.$$

证 继续使用引理 4 即得到证明.

定义 3 设 x 是任何一个实数,我们用 $[x]$ 来表示不大于 x 的最大整数. 我们用 $\{x\}$ 表示 $x-[x]$.

例如 $[4.9]=4$, 所以

$$\{4.9\}=4.9-[4.9]=0.9;$$
$$[-2.3]=-3,$$

所以

$$\{-2.3\} = -2.3 - [-2.3] = 0.7;$$

$$[-0.8] = -1,$$

所以

$$\{-0.8\} = -0.8 - [-0.8] = 0.2;$$

$$[9] = 9, \quad \{9\} = 0;$$

$$[-11] = -11, \quad \{-11\} = 0;$$

$$[\sqrt{2}] = 1, \quad \{\sqrt{2}\} = 0.41421356\cdots.$$

由定义 3 可以得到下列的性质:

(I) $x = [x] + \{x\}$, $x - 1 < [x] \leqslant x$.

(II) 当 n 是一个整数时,我们有 $[n + x] = n + [x]$.

(III) 当 $0 \leqslant x < 1$ 时,有 $[x] = 0$.

例 7 当 x 是一个实数时,我们有 $0 \leqslant \{x\} < 1$.

证 设 $x = n + y$, 其中 n 是一个整数而 $0 \leqslant y < 1$. 由 (II) 和 (III) 我们有

$$[x] = [n + y] = n + [y] = n. \tag{33}$$

由性质 (I) 和 (33) 式我们有

$$\{x\} = x - [x] = n + y - n = y. \tag{34}$$

由于 $0 \leqslant y < 1$ 和 (34) 式,我们得到 $0 \leqslant \{x\} < 1$.

如果 α 是一个无理数,则有 $\alpha = [\alpha] + \{\alpha\}$. 令 $[\alpha] = a_1$ 是一个整数,由例 7 我们有 $0 \leqslant \{\alpha\} < 1$. 但 $\{\alpha\} \neq 0$, 因为如果 $\{\alpha\} = 0$, 则由 $\alpha = [\alpha] + \{\alpha\}$ 知道 α 是一个整数而和假设 α 是一个无理数发生矛盾. 所以 $0 < \{\alpha\} < 1$. 令 $\alpha_1 = \frac{1}{\{\alpha\}}$, 则我们有 $\alpha_1 > 1$, 而

$$\alpha = a_1 + \frac{1}{\frac{1}{\{\alpha\}}} = a_1 + \frac{1}{\alpha_1}. \tag{35}$$

这里α_1是一个无理数。因为如果α_1是一个有理数,则由$\alpha_1>1$和(35)式知道α是一个有理数而和假设α是一个无理数发生矛盾. 令$[\alpha_1]=a_2$,则我们有$\alpha_1=a_2+\{\alpha_1\}$,其中$0\leqslant\{\alpha_1\}<1$. 又$\{\alpha_1\}\neq 0$,因为如果$\{\alpha_1\}=0$,则由$\alpha_1=a_2+\{\alpha_1\}$知道$\alpha_1$是一个正整数而和$\alpha_1$是一个无理数发生矛盾. 令$\alpha_2=\dfrac{1}{\{\alpha_1\}}$,则由于$0<\{\alpha_1\}<1$,我们有$\alpha_2>1$,而

$$\alpha_1=a_2+\frac{1}{\dfrac{1}{\{\alpha_1\}}}=a_2+\frac{1}{\alpha_2}. \tag{36}$$

设当$1\leqslant i\leqslant k$时,我们都有$\alpha_i=[\alpha_i]+\{\alpha_i\}$,其中$\alpha_i$是一个无理数而$0<\{\alpha_i\}<1$. 令

$$a_{i+1}=[\alpha_i],\quad \alpha_{i+1}=\frac{1}{\{\alpha_i\}}>1,$$

则当$1\leqslant i\leqslant k$时我们都有

$$\alpha_i=a_{i+1}+\frac{1}{\dfrac{1}{\{\alpha_i\}}}=a_{i+1}+\frac{1}{\alpha_{i+1}}. \tag{37}$$

又$\alpha_{k+1}=\dfrac{1}{\{\alpha_k\}}>1$,故得到$\alpha_{k+1}=[\alpha_{k+1}]+\{\alpha_{k+1}\}$,其中$0\leqslant\{\alpha_{k+1}\}<1$. 又$\{\alpha_{k+1}\}\neq 0$,因为如果$\{\alpha_{k+1}\}=0$,则由于$\alpha_{k+1}=[\alpha_{k+1}]+\{\alpha_{k+1}\}$知道$\alpha_{k+1}$是一个正整数,而由(37)式知道$\alpha_k$是一个有理数,这和$\alpha_k$是一个无理数发生矛盾. 所以$0<\{\alpha_{k+1}\}<1$. 令$a_{k+2}=[\alpha_{k+1}]$,$\alpha_{k+2}=\dfrac{1}{\{\alpha_{k+1}\}}$. 由于$\alpha_{k+2}>1$,所以我们有

$$\alpha_{k+1}=a_{k+2}+\frac{1}{\dfrac{1}{\{\alpha_{k+1}\}}}=a_{k+2}+\frac{1}{\alpha_{k+2}}. \tag{38}$$

即(37)式对于 $i=k+1$ 也成立. 所以由数学归纳法知道(37)式对于所有正整数 i 都能够成立. 由(35)和(37)式我们知道对于所有正整数 k 都有

$$\alpha=[a_1, a_2, \cdots, a_k, \alpha_k].$$

例 8 求证(3)和(4)式成立.

证 在引理 5 中我们取 $a_1=b$, $2b=a_2=a_3=a_4=a_5=\cdots$. 由(2)式我们有

$$\sqrt{b^2+1}=[b, 2b, 2b, 2b, 2b, \cdots].$$

由(2)式和定义 1 我们有

$$\frac{p_3}{q_3}=b+\cfrac{1}{2b+\cfrac{1}{2b}},$$

$$\frac{p_4}{q_4}=b+\cfrac{1}{2b+\cfrac{1}{2b+\cfrac{1}{2b}}},$$

$$\frac{p_5}{q_5}=b+\cfrac{1}{2b+\cfrac{1}{2b+\cfrac{1}{2b+\cfrac{1}{2b}}}}.$$

故由引理 5 知道(3)和(4)式都成立.

例 9 求证(16)式成立.

证 在引理 5 中我们取 $a_1=b-1$, 当 $k\geqslant 1$ 时取 $a_{2k}=1$, $a_{2k+1}=2(b-1)$. 由(13)式我们有

$\sqrt{b^2-1}=[b-1, 1, 2(b-1), 1, 2(b-1), 1, 2(b-1), \cdots]$. 由(13)式和定义 1 我们有

$$\frac{p_7}{q_7}=b-1+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)}}}}}},$$

$$\frac{p_8}{q_8}=b-1+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1}}}}}}}.$$

故由引理 5 知道 (16) 式成立.

定义 4 对于一个无限连分数 $[a_1, a_2, a_3, \cdots, a_n, \cdots]$，如果能找到二个整数 $s \geqslant 0$, $t > 0$ 使得

$$a_{s+i}=a_{s+kt+i},\quad i=1, 2, \cdots, t,\quad k=0, 1, 2, \cdots$$

成立，则我们就把这个无限连分数叫作循环连分数，并简单地把它记作 $[a_1, a_2, \cdots, a_s, \dot{a}_{s+1}, \cdots, \dot{a}_{s+t}]$.

例 10 设 b 是一个 $\geqslant 1$ 的实数，我们有

$$\sqrt{b^2+1}=[b, \dot{2b}]. \tag{39}$$

当 b 是一个 $\geqslant 2$ 的实数时，则我们有

$$\sqrt{b^2-1}=[b-1, \dot{1}, 2(\dot{b}-1)]. \tag{40}$$

证 由(2)式和定义 4，(39)式成立．由(13)式和定义 4 我们知道(40)式成立．

例 11 设 b 是一个 $\geqslant 1$ 的实数，请用引理 1 求 $[b, 2b]$ 中的 p_1 到 p_8 和 q_1 到 q_8 关于 b 的表示式．

解 在引理 1 中取 $a_1 = b$，并当 $k \geqslant 2$ 时取 $a_k = 2b$，则由引理 1 我们有

$$
\begin{aligned}
& p_1 = b,\ p_2 = 2b^2 + 1, \\
& p_3 = 2b(2b^2 + 1) + b = 4b^3 + 3b, \\
& p_4 = 2b(4b^3 + 3b) + 2b^2 + 1 = 8b^4 + 8b^2 + 1, \\
& p_5 = 2b(8b^4 + 8b^2 + 1) + 4b^3 + 3b = 16b^5 + 20b^3 + 5b, \\
& p_6 = 2b(16b^5 + 20b^3 + 5b) + 8b^4 + 8b^2 + 1 \\
& \quad = 32b^6 + 48b^4 + 18b^2 + 1, \\
& p_7 = 2b(32b^6 + 48b^4 + 18b^2 + 1) + 16b^5 + 20b^3 + 5b \\
& \quad = 64b^7 + 112b^5 + 56b^3 + 7b, \\
& p_8 = 2b(64b^7 + 112b^5 + 56b^3 + 7b) + 32b^6 + 48b^4 \\
& \qquad + 18b^2 + 1 \\
& \quad = 128b^8 + 256b^6 + 160b^4 + 32b^2 + 1;
\end{aligned}
$$

$$
\begin{aligned}
& q_1 = 1,\quad q_2 = 2b,\quad q_3 = 4b^2 + 1, \\
& q_4 = 2b(4b^2 + 1) + 2b = 8b^3 + 4b, \\
& q_5 = 2b(8b^3 + 4b) + 4b^2 + 1 = 16b^4 + 12b^2 + 1, \\
& q_6 = 2b(16b^4 + 12b^2 + 1) + 8b^3 + 4b \\
& \quad = 32b^5 + 32b^3 + 6b, \\
& q_7 = 2b(32b^5 + 32b^3 + 6b) + 16b^4 + 12b^2 + 1 \\
& \quad = 64b^6 + 80b^4 + 24b^2 + 1, \\
& q_8 = 2b(64b^6 + 80b^4 + 24b^2 + 1) + 32b^5 + 32b + 6b \\
& \quad = 128b^7 + 192b^5 + 80b^3 + 8b.
\end{aligned}
$$

例 12 求证 $\sqrt{65} = 8.0622577482\cdots$.

证 在(39)式中取 $b=8$，由引理5和在例11中取

$$\frac{p_5}{q_5}\leqslant\sqrt{65}\leqslant\frac{p_6}{q_6},$$

得到

$$\sqrt{65}\geqslant\frac{16\times 8^5+20\times 8^3+5\times 8}{16\times 8^4+12\times 8^2+1}$$

$$=\frac{534568}{66305}\geqslant 8.06225774828,$$

$$\sqrt{65}\leqslant\frac{32\times 8^6+48\times 8^4+18\times 8^2+1}{32\times 8^5+32\times 8^3+48}$$

$$=\frac{8586369}{1065008}\leqslant 8.062257748299.$$

例 13 求证 $\sqrt{2}=1.414213562373\cdots$.

证 在(39)式中取 $b=7$，由引理5和在例11中取

$$\frac{p_7}{q_7}<\sqrt{50}<\frac{p_6}{q_6},$$

得到

$$\sqrt{50}\geqslant\frac{64\times 7^7+112\times 7^5+56\times 7^3+7^2}{64\times 7^6+80\times 7^4+24\times 7^2+1}$$

$$=\frac{54608393}{7722793},$$

由于 $$5\times\sqrt{2}=\sqrt{50},$$

故得到 $$\sqrt{2}\geqslant 1.414213562373.$$

$$\sqrt{50}\leqslant\frac{32\times 7^6+48\times 7^4+18\times 7^2+1}{32\times 7^5+32\times 7^3+6\times 7}$$

$$=\frac{3880899}{548842},$$

由 $$5\times\sqrt{2}=50,$$

而得到 $$\sqrt{2}\leqslant 1.4142135623733.$$

例 14 求证 $\sqrt{26}=5.099019513592\cdots$.

证 在(39)式中取 $b=5$，在引理 5 和例 11 中取

$$\frac{p_7}{q_7}<\sqrt{26}<\frac{p_8}{q_8},$$

得到

$$\sqrt{26}\leqslant\frac{128\times5^8+256\times5^6+160\times5^4+32\times5^2+1}{128\times5^7+192\times5^5+80\times5^3+40}$$

$$=\frac{54100801}{10610040}\leqslant5.0990195135928,$$

$$\sqrt{26}\geqslant\frac{64\times5^7+112\times5^5+56\times5^3+35}{64\times5^6+80\times5^4+24\times5^2+1}$$

$$=\frac{5357035}{1050601}\geqslant5.0990195135926.$$

例 15 设 b 是一个 $\geqslant2$ 的实数，请用引理 1 求 $[b-1,\dot{1},\overline{2(b-1)}]$ 中的 p_1 到 p_{12} 和 q_1 到 q_{12}.

解 在引理 1 中取 $a_1=b-1$，而当 $k\geqslant1$ 时取 $a_{2k}=1$，$a_{2k+1}=2(b-1)$，则由引理 1 我们有

$p_1=b-1,\quad p_2=b,$

$p_3=2b(b-1)+b-1=2b^2-b-1,$

$p_4=2b^2-b-1+b=2b^2-1,$

$p_5=2(b-1)(2b^2-1)+2b^2-b-1$

$\quad=4b^3-4b^2+2b^2-2b-b+1$

$\quad=4b^3-2b^2-3b+1,$

$p_6=4b^3-2b^2-3b+1+2b^2-1=4b^3-3b,$

$p_7=2(b-1)(4b^3-3b)+4b^3-2b^2-3b+1$

$\quad=8b^4-4b^3-8b^2+3b+1,$

$p_8=8b^4-8b^2+1,$

$p_9=2(b-1)(8b^4-8b^2+1)+8b^4-4b^3-8b^2+3b+1$

$$= 16b^5 - 8b^4 - 20b^3 + 8b^2 + 5b - 1,$$

$$p_{10} = 16b^5 - 20b^3 + 5b,$$

$$p_{11} = 2(b-1)(16b^5 - 20b^3 + 5b) + 16b^5 - 8b^4 - 20b^3 + 8b^2 + 5b - 1$$

$$= 32b^5 - 16b^5 - 48b^4 + 20b^3 + 18b^2 - 5b - 1,$$

$$p_{12} = 32b^6 - 48b^4 + 18b^2 - 1;$$

$$q_1 = q_2 = 1, \quad q_3 = 2(b-1) + 1 = 2b - 1, \quad q_4 = 2b,$$

$$q_5 = 4b(b-1) + 2b - 1 = 4b^2 - 2b - 1,$$

$$q_6 = 4b^2 - 1,$$

$$q_7 = 2(b-1)(4b^2 - 1) + 4b^2 - 2b - 1$$

$$= 8b^3 - 4b^2 - 4b + 1,$$

$$q_8 = 8b^3 - 4b,$$

$$q_9 = 2(b-1)(8b^3 - 4b) + 8b^3 - 4b^2 - 4b + 1$$

$$= 16b^4 - 8b^3 - 12b^2 + 4b + 1,$$

$$q_{10} = 16b^4 - 12b^2 + 1,$$

$$q_{11} = 2(b-1)(16b^4 - 12b^2 + 1) + 16b^4 - 8b^3 - 12b^2 + 4b + 1 = 32b^5 - 16b^4 - 32b^3 + 12b^2 + 6b - 1,$$

$$q_{12} = 32b^5 - 32b^3 + 6b.$$

例 16 求证 $\sqrt{3} = 1.73205080756\cdots$.

证 在(40)式中取 $b = 7$，由引理5和例15我们有

$$\frac{p_{11}}{q_{11}} < \sqrt{48} < \frac{p_{12}}{q_{12}},$$

故得到

$$\sqrt{3} = \frac{\sqrt{48}}{4} < \frac{32 \times 7^6 - 48 \times 7^4 + 18 \times 7^2 - 1}{4(32 \times 7^5 - 32 \times 7^3 + 42)}$$

$$= \frac{3650401}{(4)(526890)} < 1.732050807569,$$

$$\sqrt{3}=\frac{\sqrt{48}}{4}$$

$$\geqslant\frac{32\times7^6-16\times7^5-48\times7^4+20\times7^3+18\times7^2-35-1}{(32\times7^5-16\times7^4-32\times7^3+12\times7^2+42-1)(4)}$$

$$=\frac{3388314}{(4)(489061)}\geqslant1.732050807567.$$

例 17 求证 $\sqrt{5}=2.236067977499\cdots$.

证 在(40)式中取 $b=9$，由引理 5 和例 15 我们有

$$\frac{p_{11}}{q_{11}}<\sqrt{80}<\frac{p_{12}}{q_{12}},$$

故得到

$$\sqrt{5}=\frac{\sqrt{80}}{4}<\frac{32\times9^6-48\times9^4+18\times9^2-1}{4(32\times9^5-32\times9^3+54)}$$

$$=\frac{16692641}{4(1866294)}<2.2360679774998,$$

$$\sqrt{5}=\frac{\sqrt{80}}{4}$$

$$>\frac{32\times9^6-16\times9^5-48\times9^4+20\times9^3+18\times9^2-46}{4(32\times9^5-16\times9^4-32\times9^3+12\times9^2+54-1)}$$

$$=\frac{15762392}{4(1762289)}>2.2360679774997.$$

例 18 求证 $\sqrt{7}=2.645751311064\cdots$.

证 在(40)式中取 $b=8$，由引理 5 和例 15 我们有

$$\frac{p_{11}}{q_{11}}<\sqrt{63}<\frac{p_{12}}{q_{12}},$$

故得到

$$\sqrt{7}=\frac{\sqrt{63}}{3}\leqslant\frac{32\times8^6-48\times8^4+18\times8^2-1}{3(32\times8^5-32\times8^3+48)}$$

$$=\frac{8193151}{3(1032240)}\leqslant2.6457513110647,$$

五乙

$$\sqrt{7}=\frac{\sqrt{63}}{3}$$

$$\geqslant \frac{32\times 8^5-16\times 8^5-48\times 8^4+20\times 8^3+18\times 8^2-41}{3(32\times 8^5-16\times 8^4-32\times 8^3+12\times 8^2+48-1)}$$

$$=\frac{7679063}{(3)(967471)}\geqslant 2.6457513110642.$$

例 19 求证 $\sqrt{11}=3.316624790355\cdots$.

证 在(40)式中取 $b=10$，由引理5和例15我们有

$$\frac{p_{11}}{q_{11}}<\sqrt{99}<\frac{p_{12}}{q_{12}},$$

故我们有

$$\sqrt{11}=\frac{\sqrt{99}}{3}\leqslant \frac{32\times 10^6-48\times 10^4+18\times 10^2-1}{3(32\times 10^5-32\times 10^3+60)}$$

$$=\frac{31521799}{9504180}\leqslant 3.3166247903555,$$

$$\sqrt{11}=\frac{\sqrt{99}}{3}$$

$$\geqslant \frac{32\times 10^6-16\times 10^5-48\times 10^4+20\times 10^3+18\times 10^2-51}{3(32\times 10^5-16\times 10^4-32\times 10^3+12\times 10^2+59)}$$

$$=\frac{29941749}{9027777}\geqslant 3.3166247903553.$$

例 20 求证 $\sqrt{13}=3.605551275\cdots$.

证 由例13和例14我们有

$$\sqrt{13}=\frac{\sqrt{26}}{\sqrt{2}}=\frac{5.099019513592\cdots}{1.414213562373\cdots}=3.605551275\cdots.$$

关于连分数的推广，请参看华罗庚、王元著《数论在近似分析中的应用》一书.

§ 6. 函数 $[x]$, $\{x\}$ 的一些性质

例 21 我们有

$$[x]+[y]\leqslant[x+y],\ \{x\}+\{y\}\geqslant\{x+y\}. \tag{41}$$

$$[-x]=\begin{cases}-[x]+1, & \text{当 } x \text{ 不是整数时;}\\ -[x], & \text{当 } x \text{ 是整数时.}\end{cases} \tag{42}$$

证 设 $x=n+a$, $y=m+b$, 其中 n 和 m 都是整数而 $0\leqslant a<1, 0\leqslant b<1$. 由定义 3 所得到的性质(II)和(III), 我们有

$$\begin{aligned}[x]+[y]&=n+m+[a]+[b]\\&=m+n\leqslant m+n+[a+b]\\&=[x+y],\end{aligned}$$

我们又有

$$\begin{aligned}\{x\}+\{y\}&=x-[x]+y-[y]\geqslant x+y-[x+y]\\&=\{x+y\},\end{aligned}$$

故 (41) 式得证. 当 x 是一个整数时, 则由定义 3 所得到的性质(II)和(III), 我们有

$$\begin{aligned}[-x]&=[-x+0]=-x+[0]=-x\\&=-(x+[0])=-[x+0]=-[x].\end{aligned}$$

当 x 不是整数时, 则令 $x=n+a$, 其中 n 是一个整数而 $0<a<1$, 则由性质 (II) 和 (III), 我们有

$$\begin{aligned}[-x]&=[-n-a]=[-n-1+1-a]\\&=-n-1+[1-a]=-n-1\\&=-[n+a]-1=-[x]-1.\end{aligned}$$

故 (42) 式得证.

例 22 设 n 是任一个正整数而 α 是一个实数时, 则有

$$[\alpha]+\left[\alpha+\frac{1}{n}\right]+\cdots+\left[\alpha+\frac{n-1}{n}\right]=[n\alpha] \tag{43}$$

成立.

证 设 $\alpha=m+a$，其中m是一个整数而 $0\leqslant a<1$，则由性质(II)我们有

$$[\alpha]+\left[\alpha+\frac{1}{n}\right]+\cdots+\left[\alpha+\frac{n-1}{n}\right]=[m+a]$$

$$+\left[m+a+\frac{1}{n}\right]+\cdots+\left[m+a+\frac{n-1}{n}\right]$$

$$=mn+[a]+\left[a+\frac{1}{n}\right]+\cdots+\left[a+\frac{n-1}{n}\right], \tag{44}$$

$$[n\alpha]=[nm+na]=mn+[na]. \tag{45}$$

设 $0\leqslant a<1/n$，这时由性质(III)我们有

$$[a]+\left[a+\frac{1}{n}\right]+\cdots+\left[a+\frac{n-1}{n}\right]=0=[na],$$

故当 $0\leqslant a<\frac{1}{n}$ 时，由(44)和(45)式知道(43)式成立。设 l 是一个正整数，它使得 $\frac{l}{n}\leqslant a<\frac{l+1}{n}\leqslant 1$ 成立。由于当 $0\leqslant i\leqslant n-l-1$ 时有 $\left[a+\frac{i}{n}\right]=0$，而当 $n-l\leqslant i\leqslant n-1$ 时有 $\left[a+\frac{i}{n}\right]=1$，故得到当 $\frac{l}{n}\leqslant a<\frac{l+1}{n}$ 时，我们有

$$[a]+\left[a+\frac{1}{n}\right]+\cdots+\left[a+\frac{n-1}{n}\right]=l=[na].$$

因而由(44)和(45)式知道(43)式成立。

例 23 设 a，b 是二个整数，$b>0$，则有

$$a=b\left[\frac{a}{b}\right]+b\left\{\frac{a}{b}\right\},\quad 0\leqslant b\left\{\frac{a}{b}\right\}\leqslant b-1.$$

证 由性质(I)我们有

$$\frac{a}{b}=\left[\frac{a}{b}\right]+\left\{\frac{a}{b}\right\},$$

故得到

$$a = b\left[\frac{a}{b}\right] + b\left\{\frac{a}{b}\right\}.$$

由例 7 和 $b > 0$，我们有 $b\left\{\frac{a}{b}\right\} \geqslant 0$. 设 $a = bm + r$，其中 m 是一个整数而 $0 \leqslant r \leqslant b - 1$，则我们有 $\frac{a}{b} = m + \frac{r}{b}$.

由性质 (II) 和性质 (III)，我们有

$$\left[\frac{a}{b}\right] = \left[m + \frac{r}{b}\right] = m + \left[\frac{r}{b}\right] = m,$$

因而由性质 (I) 我们有

$$\left\{\frac{a}{b}\right\} = \frac{a}{b} - \left[\frac{a}{b}\right] = m + \frac{r}{b} - m = \frac{r}{b}.$$

使用 $0 \leqslant r \leqslant b - 1$，即得到 $b\left\{\frac{a}{b}\right\} \leqslant b - 1$.

例 24 我们有

$$[2x] + [2y] \geqslant [x] + [y] + [x + y].$$

证 设 $x = m + a$，其中 m 是一个整数而 $0 \leqslant a < 1$；$y = n + b$，其中 n 是一个整数而 $0 \leqslant b < 1$. 当 $a \geqslant b$ 时，我们由性质 (II) 和性质 (III) 有

$$\begin{aligned}[2x] + [2y] &= [2m + 2a] + [2n + 2b] = 2m + 2n \\ &\quad + [2a] + [2b] \geqslant m + n + m + n + [a + b] \\ &= [m + a] + [n + b] + [m + n + a + b] \\ &= [x] + [y] + [x + y].\end{aligned}$$

同理，对于 $a < b$ 上式也成立，故例 24 得证.

§7. 数 论 函 数

在前面，我们曾经提出了几种在数论里常用到的函数，例如欧拉函数 $\varphi(n)$，函数 $[x]$，$\{x\}$，这些函数都可以叫作数论

函数．所谓数论函数一般是指在整数(或正整数)上有确定的数值的函数．在本节中我们还要再讨论几种数论函数．

设 a 是一个正整数而 b 是一个整数，如果存在一个正整数 m 使得 $a=bm$ 成立，我们就把 b 叫作 a 的因数．例如 16 的因数是 1，2，4，8，16 共有 5 个，而 12 的因数是 1，2，3，4，6，12 共有 6 个．

定义 5 如果 n 是一个正整数，我们用 $d(n)$ 来表示 n 的因数的个数，例如 $d(16)=5$，$d(12)=6$．我们把 $d(n)$ 叫作除数函数．

引理 6 设 $n=p_1^{\alpha_1}\cdots p_m^{\alpha_m}$，
其中 $p_1,\cdots,p_m$ 都是不同的素数，而 $\alpha_1,\cdots,\alpha_m$ 都是正整数，则我们有

$$d(n)=(\alpha_1+1)\cdots(\alpha_m+1).$$

证 n 的任何一个因数的形式是

$$p_1^{\beta_1}\cdots p_m^{\beta_m}.$$

这里有

$$0\leqslant\beta_1\leqslant\alpha_1,$$
$$\cdots\cdots\cdots\cdots,$$
$$0\leqslant\beta_m\leqslant\alpha_m.$$

由于 β_1 可以经过 α_1+1 个不同的整数，……，β_m 可以经过 α_m+1 个不同的整数，而且每个 β_i 所经过的整数可以同其它 β_j 所经过的整数进行任意的配合，这样就可以产生 $(\alpha_1+1)\cdots(\alpha_m+1)$ 个不同的正整数，而这些正整数都是 n 的因数，所以有 $d(n)=(\alpha_1+1)\cdots(\alpha_m+1)$．

引理 7 设 a，b 是二个正整数而 $(a,b)=1$，则我们有

$$d(ab)=d(a)d(b).$$

证 设 $a=p_1^{\alpha_1}\cdots p_n^{\alpha_n}$，$b=q_1^{\beta_1}\cdots q_m^{\beta_m}$，
其中 $p_1,\cdots,p_n,q_1,\cdots,q_m$ 都是素数而 $\alpha_1,\cdots,\alpha_n,\beta_1,\cdots,\beta_m$

都是正整数. 由于 $(a, b)=1$，我们知道这时任何一个 $p_i(i=1,\cdots,n)$ 与任何一个 $q_j(j=1,\cdots,m)$ 都不能相等，故由引理 6 我们有

$$d(ab)=d(p_1^{\alpha_1}\cdots p_n^{\alpha_n}q_1^{\beta_1}\cdots q_m^{\beta_m})$$
$$=(\alpha_1+1)\cdots(\alpha_n+1)(\beta_1+1)\cdots(\beta_m+1). \quad (46)$$

又由引理 6 我们有

$$d(a)d(b)=d(p_1^{\alpha_1}\cdots p_n^{\alpha_n})d(q_1^{\beta_1}\cdots q_m^{\beta_m})$$
$$=(\alpha_1+1)\cdots(\alpha_n+1)(\beta_1+1)\cdots(\beta_m+1). \quad (47)$$

由 (46) 和 (47) 式引理7得证.

例 25 求 $d(3496)=?$

解 因为 $3496=2^3\times 19\times 23$，所以由引理 6 我们有

$$d(3496)=(3+1)(1+1)(1+1)=16.$$

定义 6 如果 n 是一个正整数，则我们把 n 的所有因数相加以后所得到的和叫作 n 的因数和，记作 $\sigma(n)$.

例如 32 的因数是 1, 2, 4, 8, 16, 32, 所以 32 的因数和是

$$\sigma(32)=1+2+4+8+16+32=63.$$

由于 24 的因数是 1, 2, 3, 4, 6, 8, 12, 24, 所以 24 的因数和是

$$\sigma(24)=1+2+3+4+6+8+12+24=60.$$

引理 8 当 l, m 是正整数且 $m\geqslant 2$ 时，我们有

$$1+m+\cdots+m^l=\frac{m^{l+1}-1}{m-1}. \quad (48)$$

证 当 $l=1$ 时，我们有

$$1+m=\frac{(m+1)(m-1)}{m-1}=\frac{m^2-1}{m-1},$$

故当 $l=1$ 时本引理成立. 现设 $k\geqslant 2$，而当 l 等于 $1, 2, \cdots, k-1$ 时本引理都成立，则我们有

$$1+m+\cdots+m^{k-1}+m^k=\frac{m^k-1}{m-1}+m^k$$

$$= \frac{m^{k+1}-1}{m-1}.$$

故当 $l=k$ 时本引理也成立. 由数学归纳法知道引理 8 成立.

引理 9 设 p 是一个素数而 l 是一个正整数,则我们有

$$\sigma(p^l) = \frac{p^{l+1}-1}{p-1}.$$

证 由于 p^l 的因数是 $1, p, \cdots, p^{l-1}, p^l$, 所以我们有

$$\sigma(p^l) = 1 + p + \cdots + p^l.$$

而由引理 8 知道本引理成立.

引理 10 如果 m 是一个正整数而 $n = p_1^{\alpha_1}\cdots p_m^{\alpha_m}$, 其中 $p_1, \cdots, p_m$ 是 m 个不同的素数, $\alpha_1, \cdots, \alpha_m$ 是 m 个正整数,则我们有

$$\sigma(n) = \frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_m^{\alpha_m+1}-1}{p_m-1}.$$

证 当 $m=1$ 时,由引理 9 知道本引理成立. 当 $m=2$ 时,则有 $n = p_1^{\alpha_1}p_2^{\alpha_2}$. 令 $p_1^0 = p_2^0 = 1$. 如果将 $1 + p_1 + \cdots + p_1^{\alpha_1}$ 中的数 p_1^i (其中 $i = 0, 1, \cdots, \alpha_1$) 同 $1 + p_2 + \cdots + p_2^{\alpha_2}$ 中的数 p_2^j (其中 $j = 0, 1, \cdots, \alpha_2$) 一一相乘,这时 $n = p_1^{\alpha_1}p_2^{\alpha_2}$ 的全体因数都能够出现而且每个因数正好只出现一次, 所以有

$$\sigma(n) = (1 + p_1 + \cdots + p_1^{\alpha_1})(1 + p_2 + \cdots + p_2^{\alpha_2}). \quad (49)$$

故当 $m=2$ 时, 由引理 8 和 (49) 式知道本引理成立. 现设 $m \geqslant 3$. 如果将

$$(1 + p_1 + \cdots + p_1^{\alpha_1})(1 + p_2 + \cdots + p_2^{\alpha_2})\cdots (1 + p_m + \cdots + p_m^{\alpha_m}) \quad (50)$$

展开,则出现的都是 n 的因数, 又 n 的全体因数都能出现, 而且每个因数只出现一次,故由 (50) 式和引理 8 我们有

$$\sigma(n) = \frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_m^{\alpha_m+1}-1}{p_m-1},$$

即本引理成立.

例 26 求 $\sigma(450)=?$

解 因为 $450=2\times3^2\times5^2$，所以由引理 10 我们有

$$\sigma(450)=\frac{2^2-1}{2-1}\cdot\frac{3^3-1}{3-1}\cdot\frac{5^3-1}{5-1}$$
$$=3\times13\times31=1209.$$

引理 11 设 m,n 是二个正整数且 $(m,n)=1$，则我们有

$$\sigma(mn)=\sigma(m)\cdot\sigma(n).$$

证 设 $m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，$n=q_1^{\beta_1}\cdots q_l^{\beta_l}$，
其中 $p_1,\cdots,p_k$，是 k 个不同的素数，$q_1,\cdots,q_l$ 是 l 个不同的素数，而 $\alpha_1,\cdots,\alpha_k,\beta_1,\cdots,\beta_l$ 都是正整数. 由于 $(m,n)=1$，故任何 p_i（其中 $i=1,\cdots,k$）与任何 q_j（其中 $j=1,\cdots,l$）都不相同. 所以由引理 10 我们有

$$\sigma(mn)=\sigma(p_1^{\alpha_1}\cdots p_k^{\alpha_k}\cdot q_1^{\beta_1}\cdots q_l^{\beta_l})$$
$$=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_k^{\alpha_k+1}-1}{p_k-1}\cdot\frac{q_1^{\beta_1+1}-1}{q_1-1}\cdots\frac{q_l^{\beta_l+1}-1}{q_l-1}. \tag{51}$$

由引理 10 我们有

$$\sigma(m)\cdot\sigma(n)=\sigma(p_1^{\alpha_1}\cdots p_k^{\alpha_k})\cdot\sigma(q_1^{\beta_1}\cdots q_l^{\beta_l})$$
$$=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_k^{\alpha_k+1}-1}{p_k-1}\cdot\frac{q_1^{\beta_1+1}-1}{q_1-1}\cdots\frac{q_l^{\beta_l+1}-1}{q_l-1}. \tag{52}$$

由 (51) 和 (52) 式本引理得证.

定义 7 如果 n 是一个正整数，则我们把除去 n 本身以外的 n 的因数都叫作 n 的真因数.

6 的真因数是 1，2，3，而 $1+2+3$ 恰好等于 6. 28 的真因数是 1，2，4，7，14，而 $1+2+4+7+14$ 也恰好等于

28. 又 496 的真因数是 1, 2, 4, 8, 16, 31, 62, 124, 248, 而 $1+2+4+8+16+31+62+124+248=496$.

定义 8 如果 n 是一个正整数, 当我们把 n 的所有真因数相加以后,所得到的和恰好等于 n 时,则我们把 n 叫作完全数. 或者说当 $\sigma(n)=2n$ 成立时,则我们把 n 叫作完全数.

例如 6, 28, 496 都是完全数.

引理 12 如果 n 是一个 $\geqslant 2$ 的整数而 2^n-1 是一个素数,则

$$2^{n-1}(2^n-1)$$

是一个完全数.

证 因为 $(2^{n-1}, 2^n-1)=1$ 成立,所以由引理 11 我们有

$$\sigma(2^{n-1}(2^n-1))=\sigma(2^{n-1})\cdot\sigma(2^n-1). \tag{53}$$

因为 2^n-1 是一个素数,所以 2^n-1 的因数是 $1, 2^n-1$,故得到

$$\sigma(2^n-1)=2^n-1+1=2^n. \tag{54}$$

由于 $n\geqslant 2$, 故由引理 9 我们有

$$\sigma(2^{n-1})=\frac{2^n-1}{2-1}=2^n-1. \tag{55}$$

由 (53) 到 (55) 式我们有

$$\sigma(2^{n-1}(2^n-1))=(2^n-1)\cdot 2^n=2\cdot 2^{n-1}(2^n-1),$$

所以 $2^{n-1}(2^n-1)$ 是一个完全数.

由于 $2^7-1=127$ 是一个素数, 所以 $2^6\cdot(2^7-1)=64\times 127=8128$ 是一个完全数. 由于 $2^{13}-1=8191$ 是一个素数,所以 $2^{12}\cdot(2^{13}-1)=4096\times 8191=33550336$ 也是一个完全数. 上面求得的完全数, 例如 6, 28, 496, 8128, 33550336 等都是偶数. 直到现在我们还没有找到一个完全数是奇数的.

定义 9 如果 n 是一个正整数而 λ 是一个非负整数, 则

令

$$\sigma_\lambda(n)=\sum_{d|n}d^\lambda.$$

这里 $\sum_{d|n}$ 系表示一个和式而和式中的 d 经过 n 的所有因数.

设 m 是一个整数，令 $m^0=1$. 由定义 5 和定义 9 我们有

$$\sigma_0(n)=d(n).$$

由定义 6 和定义 9 我们有

$$\sigma_1(n)=\sigma(n).$$

例 27 求 $\sigma_2(28)=?$

解 由于 28 的因数是 1, 2, 4, 7, 14, 28, 所以有

$$\sigma_2(28)=1+2^2+4^2+7^2+14^2+28^2=1050.$$

例 28 求 $\sigma_3(62)=?$

解 由于 62 的因数是 1, 2, 31, 62, 所以有

$$\sigma_3(62)=1+2^3+31^3+62^3=268128.$$

定义 10 麦比乌斯（Möbius）函数 $\mu(n)$ 是一个数论函数，它的定义是这样的：

$$\mu(n)=\begin{cases}1, & \text{当 } n=1 \text{ 时；}\\ (-1)^r, & \text{当 } n \text{ 是 } r \text{ 个不同的素数的乘积时；}\\ 0 & \text{当 } n \text{ 能被一个素数的平方除尽时.}\end{cases}$$

由定义容易算出

$\mu(1)=1$, $\mu(2)=-1$, $\mu(3)=-1$, $\mu(4)=0$,
$\mu(5)=-1$, $\mu(6)=1$, $\mu(7)=-1$, $\mu(8)=0$,
$\mu(9)=0$, $\mu(10)=1$, $\mu(11)=-1$, $\mu(12)=0$,
$\mu(13)=-1$, $\mu(14)=1$.

又当 p 是一个素数时，则有 $\mu(p)=-1$.

引理 13 如果 m, n 是二个正整数而 $(m,n)=1$，则我们有

$$\mu(mn)=\mu(m)\cdot\mu(n).$$

证 如果m或n能被一个素数的平方除尽，则mn也能够被这个素数的平方除尽．故得到

$$\mu(mn)=0=\mu(m)\cdot\mu(n).$$

如果任何一个素数的平方都不能除尽m，也不能够除尽n，则由于$(m,n)=1$而得到任何一个素数的平方都不能够除尽mn．设m有a个不同的素因数，而n有b个不同的素因数，则由于$(m,n)=1$知道mn有$a+b$个不同的素因数．故得到

$$\mu(mn)=(-1)^{a+b}=(-1)^a(-1)^b=\mu(m)\cdot\mu(n).$$

引理 14 我们有

$$\sum_{d|n}\mu(d)=\begin{cases}1, 当 n=1 时;\\ 0, 当 n>1 时.\end{cases}$$

证 当$n=1$时，则由于$\sum\limits_{d|n}\mu(d)=\mu(1)=1$，故本引理成立．

现设$n\geqslant 2$是一个整数．当m是一个正整数而$m|n$时，我们使用记号$\sum\limits_{m|d|n}$来表示一个和式，和式中的d经过所有能够被m除尽的n的因数．特别当$m=1$时，则$\sum\limits_{1|d|n}$相同于$\sum\limits_{d|n}$．现在设p是一个素数，则我们有

$$\sum_{d|p}\mu(d)=1+\mu(p)=1-1=0. \tag{56}$$

现在设$p_1,\cdots,p_l$是l个不同的素数，我们首先来证明

$$\sum_{d|p_1\cdots p_l}\mu(d)=0 \tag{57}$$

成立．当$l=1$时，由(56)式知道(57)式成立，现在设$k\geqslant 2$而当$l=1,\cdots,k-1$时(57)式都成立，即

$$\sum_{d \mid p_1 \cdots p_{k-1}} \mu(d) = 0, \tag{58}$$

则由 $p_1, \cdots, p_k$ 是 k 个不同的素数和引理 13，我们有

$$\sum_{d \mid p_1 \cdots p_k} \mu(d) = \sum_{d \mid p_1 \cdots p_{k-1}} \mu(d) + \sum_{p_k \mid d \mid p_1 \cdots p_k} \mu(d)$$

$$= (1 + \mu(p_k)) \sum_{d \mid p_1 \cdots p_{k-1}} \mu(d) = 0.$$

故当 $l = k$ 时 (57) 式也成立，而由数学归纳法知道 (57) 式成立。

设 $n = p_1^{\alpha_1} \cdots p_l^{\alpha_l}$，其中 $p_1, \cdots, p_l$ 是 l 个不同的素数，而 $\alpha_1, \cdots, \alpha_l$ 是 l 个正整数. 由于当 d 能够被一个素数的平方除尽时有 $\mu(d) = 0$. 由 (57) 式我们有

$$\sum_{d \mid n} \mu(d) = \sum_{d \mid p_1 \cdots p_l} \mu(d) = 0.$$

故本引理得证.

引理 15 设 $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$，其中 $p_1, \cdots, p_m$ 是 m 个不同的素数，而 $\alpha_1, \cdots, \alpha_m$ 都是正整数，则我们有

$$\sum_{d \mid n} |\mu(d)| = 2^m.$$

证 由于当 d 能够被一个素数的平方除尽时有 $\mu(d) = 0$，故得到

$$\sum_{d \mid n} |\mu(d)| = \sum_{d \mid p_1 \cdots p_m} |\mu(d)|. \tag{59}$$

我们将证明当 $m \geqslant 1$ 时有

$$\sum_{d \mid p_1 \cdots p_m} |\mu(d)| = 2^m \tag{60}$$

成立. 当 $m = 1$ 时由于

$$\sum_{d \mid p} |\mu(d)| = 1 + |\mu(p)| = 2,$$

故(60)式成立. 现设 $k \geqslant 2$, 而当 $m=1, \cdots, k-1$ 时(60)式都能够成立, 则由于 $p_1, \cdots, p_k$ 是 k 个不同的素数和引理 13 我们有

$$\sum_{d \mid p_1 \cdots p_k} |\mu(d)| = \sum_{d \mid p_1 \cdots p_{k-1}} |\mu(d)| + \sum_{p_k \mid d \mid p_1 \cdots p_k} |\mu(d)|$$

$$= (1 + |\mu(p_k)|) \sum_{d \mid p_1 \cdots p_{k-1}} |\mu(d)| = 2^k.$$

故当 $m=k$ 时(60)式也成立, 而由数学归纳法知道(60)式成立. 由(59)和(60)式知道引理15成立.

习　　题

1. 用数学归纳法证明:

(i) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1)$

$$= \frac{1}{3} n(n+1)(n+2).$$

(ii) $1^3 + 2^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2.$

(iii) n 是非负整数时, $a^{n+2} + (a+1)^{2n+1}$ 含有因子 $a^2 + a + 1$.

(iv) $(a_1 a_2 \cdots a_n)^{1/n} \leqslant \frac{a_1 + a_2 + \cdots + a_n}{n}$,

这里 $a_1, a_2, \cdots, a_n$ 是非负实数.

2. 将下列有理分数化成连分数:

(i) $\frac{50}{13}$, (ii) $-\frac{53}{25}$.

3. 用连分数计算 $\sqrt{41}$ 的近似值.

4. 已知 π 的连分数是

$$\pi = [3, 7, 15, 1, 292, 1, 1, \cdots],$$

试求它的最初七个渐近分数，并求其近似值。

5. 假设二元一次整系数方程 $ax+by=c$，$a>0$，且 $(a,|b|)=1$，$\frac{a}{|b|}$ 的渐近分数共有 k 个。

试证：

$$\begin{cases} x_0=(-1)^k c q_{k-1}, \\ y_0=(-1)^{k+1} c p_{k-1}\cdot\frac{|b|}{b} \end{cases}$$

是它的一组解。这里 $\frac{p_{k-1}}{q_{k-1}}$ 是 $\frac{a}{b}$ 的第 $k-1$ 个渐近分数。

6. 利用上题的结果求下列方程的整数解：

(i) $43x+15y=8$。

(ii) $10x-37y=3$。

7. 证明：

(i) $\sum_{k=1}^{n}\left[\frac{k}{2}\right]=\left[\frac{n^2}{4}\right]$。

(ii) $\sum_{k=1}^{n}\left[\frac{k}{3}\right]=\left[\frac{n(n-1)}{6}\right]$。

(iii) 当 $0<a<8$ 时，必存在整数 b 使得

$$\sum_{k=1}^{n}\left[\frac{k}{a}\right]=\left[\frac{(2n+b)^2}{8a}\right].$$

8. 证明：当 n 是正整数时

$$[\sqrt{n}+\sqrt{n+1}]=[\sqrt{4n+2}].$$

9. 设 $f(x)=x-[x]-\frac{1}{2}$，证明：

$$\sum_{k=0}^{n-1} f\left(x+\frac{k}{n}\right)=f(nx).$$

10. 试证：$d(n)$ 是奇数的充分必要条件是 n 为一个平方

数.

11. 试证: $\prod_{t|n} t = n^{d(n)/2}$,

这里 $\prod_{t|n} t$ 表示 n 的所有因数的乘积.

12. 试证: $\sum_{d^2|n} \mu(d) = \mu^2(n)$.

13. 设若 $F(n) = \sum_{d|n} f(d)$,

则有 $f(n) = \sum_{d|n} F\left(\frac{n}{d}\right)\mu(d)$, 反之亦成立.

14. 设整数 $n > 0$, 试证:

(i) $n = \sum_{d|n} \varphi(d)$.

(ii) $\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$.

15. 证明偶完全数必有 $2^{n-1}(2^n - 1)$ 的形式,并且 $2^n - 1$ 是素数.

16. 设 p, q 是两个互素的奇正整数,证明

$$\sum_{0<l<\frac{q}{2}} \left[\frac{p}{q} l\right] + \sum_{0<k<\frac{p}{2}} \left[\frac{q}{p} k\right] = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

第八章　关于复数和三角和的概念

§1. 复数的引入

如果我们只限于在实数范围内，方程

$$x^2+1=0 \tag{1}$$

没有根，则我们不可能找到一个实数 a，使得

$$a^2+1=0$$

成立．因为正数乘正数得到的是正数，负实数乘负实数得到的也是正数，即当 a 是实数时，a^2 永远是正的，所以 a^2+1 永远不为 0．由此可见，我们必须引进与实数截然不同的新的数，才能使 (1) 式有根．我们引进

$$i^2=-1. \tag{2}$$

这里 i 是不同于实数的新的数，它是 (1) 式的一个根，我们把它叫作单位纯虚数．

采用实数中的乘幂的记法，可以得到

$$i^2=-1,\quad i^3=i(i^2)=-i,\quad i^4=(i^2)(i^2)=1. \tag{3}$$

我们规定 $i^0=1$．当 k 是一个正整数时，我们使用相同于(3)式中的计算方法可以得到

$$i^{4k}=1,\quad i^{4k+1}=i,\quad i^{4k+2}=-1,\quad i^{4k+3}=-i. \tag{4}$$

我们把形如

$$z=a+bi \tag{5}$$

的数叫作复数，其中 a, b 都是实数而 i 满足 (2) 式(有时我们把 i 记作 $\sqrt{-1}$)；a 叫作复数 z 的实数部，bi 叫作复数 z 的虚部，b 叫作虚部系数，i 叫作单位纯虚数．当 $b=0$ 时，由

(5)式得到 $z=a$，就是实数 a，所以实数是复数中的一部分. 当 $a=0$ 时，由(5)式得到 $z=bi$，如果 $b\neq 0$，我们把 $z=bi$ 叫作纯虚数.

在实践中我们发现，复数的加减法可以按照代数式 $a+bx$ 的加减规则来作，即：实数部和实数部相加(减)，虚部和虚部相加(减).

例如

$$(104+11i)+(1001+103i)=(104+1001)+(11+103)i=1105+114i,$$

$$(1003+104i)-(1002-1000i)=(1003-1002)+(104+1000)i=1+1104i.$$

两个复数

$$z_1=a_1+b_1i,\quad z_2=a_2+b_2i$$

相加的规则是

$$z_1+z_2=(a_1+b_1i)+(a_2+b_2i)=(a_1+a_2)+(b_1+b_2)i. \tag{6}$$

两个复数

$$z_1=a_1+b_1i,\quad z_2=a_2+b_2i$$

相减的规则是

$$z_1-z_2=(a_1+b_1i)-(a_2+b_2i)=(a_1-a_2)+(b_1-b_2)i. \tag{7}$$

两个复数 $z_1=a_1+b_1i$ 和 $z_2=a_2+b_2i$，只有当它们的实数部和虚部分别相等时，才称这两个复数相等，如果 $z_1=z_2$，那么 $a_1=a_2$，$b_1=b_2$；反过来也对.

复数 $z=0$ 的意思是指 $a=b=0$；反过来．如果 $a=b=0$，那么 $z=0$.

例 1 已知 $(5x+\sqrt{3})-i=3+(\sqrt{2}-y)i$，$x$ 和 y 都是实数，求 x 和 y.

解 根据复数相等的条件得到

$$\begin{cases}5x+\sqrt{3}=3, \\ -1=\sqrt{2}-y.\end{cases}$$

所以 $x=\dfrac{3-\sqrt{3}}{5}$， $y=1+\sqrt{2}$.

复数 $z=a+bi$ 的绝对值(有时也叫作模)就是指正的实数 $\sqrt{a^2+b^2}$. 我们用 $|a+bi|$ 来表示 z 的绝对值，因此有

$$|a+bi|=\sqrt{a^2+b^2}. \tag{8}$$

例如

$$|3+4i|=\sqrt{3^2+4^2}=5;$$

$$\left|\frac{-1+\sqrt{3}i}{2}\right|=\sqrt{\frac{1}{4}+\frac{3}{4}}=1.$$

我们把复数 $a-bi$ 叫作复数 $z=a+bi$ 的共轭复数，记作

$$\bar{z}=a-bi. \tag{9}$$

我们也把复数 $z=a+bi$ 叫作复数 $a-bi$ 的共轭复数.

由于

$$|a+bi|=\sqrt{a^2+b^2},\quad |a-bi|=\sqrt{a^2+(-b)^2}$$
$$=\sqrt{a^2+b^2},$$

所以互为共轭的两个复数的绝对值相等.

两个复数相乘，可以按代数式 $a+bx$ 的乘法规则来进行，只要把 i^2 换成实数就可以，例如

$$\begin{aligned}(a+bi)(c+di)&=ac+adi+bci+bdi^2\\&=ac+adi+bci-bd\\&=(ac-bd)+(ad+bc)i.\end{aligned} \tag{10}$$

两个复数相除，可以先把它写成分式的形式，然后分子、分母同乘以分母的共轭复数，转化为相乘的运算，再化简. 如

计算

$$(a+bi)\div(c+di),$$

应该先把它写成 $\frac{a+bi}{c+di}$（c、d 不能同时为 0）。

$$\frac{a+bi}{c+di}=\frac{(a+bi)(c-di)}{(c+di)(c-di)}=\frac{(ac+bd)+(bc-ad)i}{c^2+d^2}$$

$$=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}i. \tag{11}$$

例 2 计算 $(1+2i)\div(3-4i)$.

解 $(1+2i)\div(3-4i)=\frac{1+2i}{3-4i}=\frac{(1+2i)(3+4i)}{(3-4i)(3+4i)}$

$$=\frac{3+4i+6i+8i^2}{9+12i-12i-16i^2}=\frac{(3-8)+(4+6)i}{9+16}$$

$$=\frac{-5+10i}{25}=\frac{-1+2i}{5}.$$

设 $z_1, z_2, \cdots, z_n$ 是 n 个复数，为方便起见，以后用求和记号 $\sum_{k=1}^{n}$ 来表示 n 个数之和，例如

$$\sum_{k=1}^{n} z_k=z_1+z_2+\cdots+z_n.$$

由 (3) 和 (4) 式我们有

$$\sum_{k=1}^{8} i^k=i+i^2+i^3+i^4+i^5+i^6+i^7+i^8$$

$$=i-1-i+1+i-1-i+1=0.$$

例 3 设 n 是一个 $\geqslant 2$ 的整数而 $z_1, z_2, \cdots, z_n$ 是 n 个复数，则我们有

$$|z_1z_2\cdots z_n|=|z_1|\cdot|z_2|\cdots|z_n|.$$

证 设 $z_1=a+bi$，$z_2=c+di$ 是二个复数，由 (10) 式我们有

$$|z_1z_2| = \sqrt{(ac-bd)^2+(ad+bc)^2}, \quad |z_1| = \sqrt{a^2+b^2},$$
$$|z_2| = \sqrt{c^2+d^2},$$

其中$|z_1z_2|$，$|z_1|$，$|z_2|$都是正数．我们又有

$$\begin{aligned}(|z_1z_2|)^2 &= (ac-bd)^2+(ad+bc)^2 \\ &= a^2c^2+b^2d^2+a^2d^2+b^2c^2 \\ &= (a^2+b^2)(c^2+d^2) = (|z_1||z_2|)^2.\end{aligned}$$

故当 $n=2$ 时例 3 成立． 现在设 $k \geqslant 3$，而当 n 等于 2，3，$\cdots$，$k-1$ 时例 3 都成立，则我们有

$$\begin{aligned}|z_1z_2\cdots z_{k-1}z_k| &= |z_1||z_2|\cdots|z_{k-2}||z_{k-1}z_k| \\ &= |z_1||z_2|\cdots|z_k|,\end{aligned}$$

故当 $n=k$ 时例 3 也成立，故由数学归纳法知道例 3 成立．

例 4 设 z_1 和 z_2 是二个复数，则我们有 $|z_1+z_2| \leqslant |z_1|+|z_2|$．

证 设 $z_1 = a+bi$，$z_2 = c+di$，其中 a，b，c，d 都是实数，则我们有

$$\begin{aligned}&(|z_1|+|z_2|)^2 - |z_1+z_2|^2 \\ &= (\sqrt{a^2+b^2}+\sqrt{c^2+d^2})^2-(a+c)^2-(b+d)^2 \\ &= a^2+b^2+c^2+d^2+2\sqrt{a^2+b^2}\cdot\sqrt{c^2+d^2} \\ &\quad -a^2-c^2-2ac-2bd-b^2-d^2 \\ &= 2(\sqrt{a^2+b^2}\cdot\sqrt{c^2+d^2}-ac-bd).\end{aligned}$$

由于

$$(a^2+b^2)(c^2+d^2)-(ac+bd)^2 = (bc-ad)^2 \geqslant 0,$$

故得到

$$(|z_1|+|z_2|)^2 - |z_1+z_2|^2 \geqslant 0.$$

由于$|z_1|$，$|z_2|$和$|z_1+z_2|$都是正数，故例 4 得证．

§ 2. 角的概念，正弦函数和余弦函数

我们可以把角看作是一条射线在平面内绕着它的端点旋转而生成的．射线旋转的开始位置叫作角的始边，射线旋转的终止位置叫作角的终边．

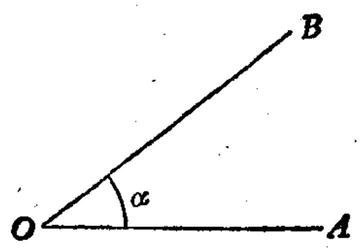


图 1

如图 1 中，OA 是角 α 的始边，OB 是角 α 的终边．

在直角坐标系中，通常取正 x 轴为角的始边，原点为角的顶点．为了区别射线绕原点旋转的两个方向，按反时针方向转成的角作为正角．

关于角的度量方法有二种不同的单位，在数论和高等数学中都采用弧度制，所以我们只介绍弧度制(因为弧度制是采用十进制的，使用起来较方便)．

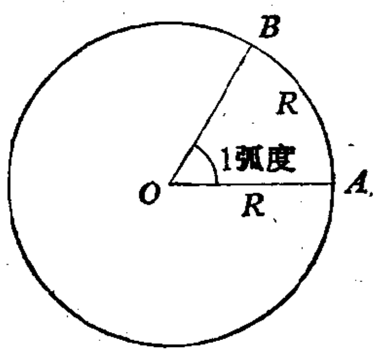


图 2

我们把等于半径长的圆弧所对的圆心角，叫作 1 弧度的角．例如，在图 2 中，弧 AB (即 $\overset{\frown}{AB}$) 的长度等于 R，而半径 OA 的长度也等于 R，这时我们说 $\angle AOB$ 就是 1 弧度的角．用弧度作单位来度量弧或角的制度，叫作弧度制．

为了方便起见，我们可以取半径 R 等于1．这时如果弧的长度等于 l，那么，这个弧所对的圆心角 α 的弧度数，也等于 l，即

$$\alpha = l.$$

在用弧度来度量角时，“弧度”二字通常略去不写．例如 $\angle AOB = 1$ 弧度，可以写成 $\angle AOB = 1$；如果 $\alpha = \frac{\pi}{4}$ 弧

度(这里我们定义半径为 $\frac{1}{2}$ 的圆的圆周的长度等于 π)，就可以写成 $\alpha = \frac{\pi}{4}$.

由于半径 R 等于 1 时，圆的圆周长度等于 2π，因此整个圆周所对的圆心角就是 2π 弧度，而在角度制中是 $360°$. 因此，可以得到

$$360° = 2\pi \text{ 弧度}, \quad \text{又} \ \pi = 3.14159265\cdots.$$

由此可以推出:

角　　度	360°	270°	180°	90°	60°	45°	30°	0°
弧　　度	2π	$\frac{3\pi}{2}$	π	$\frac{\pi}{2}$	$\frac{\pi}{3}$	$\frac{\pi}{4}$	$\frac{\pi}{6}$	0

因为 $180° = \pi$ 弧度，所以

$$1° = \frac{\pi}{180} \text{弧度} \approx 0.017453292 \text{弧度}.$$

$$1 \text{ 弧度} = \frac{180°}{\pi} \approx 57°17'44.8''.$$

角度制与弧度制是采用不同单位的度量制，利用上面的关系式，就可以进行角度与弧度的换算.

例 5　把 $67°30'$ 化成弧度.

解　因为　$67°30' = 67\frac{1}{2}$ 度，

所以　$67°30' = \frac{\pi}{180}$ 弧度 $\times 67\frac{1}{2}$

$= \frac{135\pi}{360}$ 弧度 $= \frac{3}{8}\pi$ 弧度.

例 6　把 $\frac{3}{5}\pi$ 弧度化成度.

解 $\frac{3}{5}\pi$ 弧度 $= \frac{180^\circ}{\pi} \times \frac{3}{5}\pi = 108^\circ$.

注意：以后"弧度"二字都略去，例如我们写 α 就表示 α 弧度.

设一条射线从始边转到终边，形成的角是 α（如图 3）．如果从 α 角再按反时针方向转一圈，得到 $2\pi+\alpha$ 的角；转两圈，得到 $4\pi+\alpha$ 的角；……；一般地从 α 角再按反时针方向转 n 圈，得到 $2n\pi+\alpha$ 的角，类似地，从 α 角再按顺时针方向转 n 圈，得到 $-2n\pi+\alpha$ 的角.

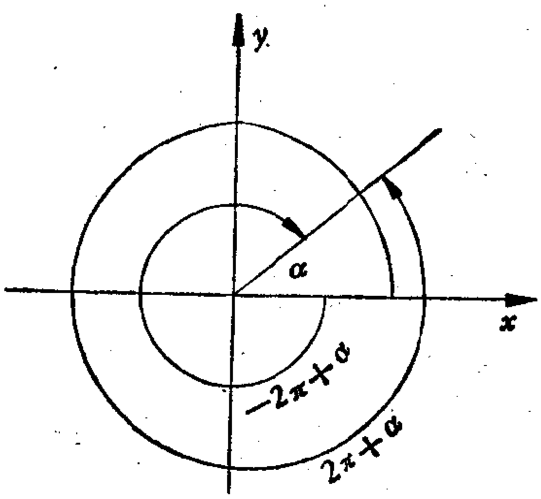


图 3

值得注意的是，这些角都有相同的始边和终边．换句话说：对于同一条终边（注意始边总是取在正 x 轴），可以形成下述形式的任意转角：

$$2n\pi+\alpha \quad (n=0, \pm 1, \pm 2, \cdots).$$

n 取正值时，表示反时针方向旋转；n 取负值时，表示顺时针方向旋转.

定义 1 在直角坐标系中，设 α 是顶点在原点，始边为正 x 轴的任意角，A 为它的终边上任一点，$OA=r$，A 的纵坐标为 y，我们把 $\frac{y}{r}$ 叫作 α 的正弦函数，记作 $\sin\alpha$，即

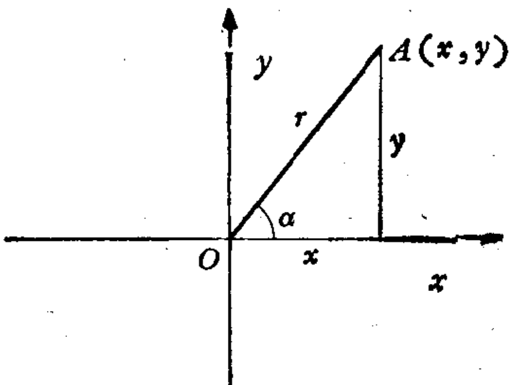


图 4

$$\sin\alpha = \frac{y}{r}.$$

定义 2 在直角坐标系中，设α是顶点在原点，始边为正x轴的任意角，A为它的终边上任一点，$OA=r$，A的坐标为(x,y)，我们把$\frac{x}{r}$叫作α的余弦函数，记作$\cos\alpha$，即

$$\cos\alpha=\frac{x}{r}.$$

我们容易证明下面的八个公式都成立（请参见高中一年级的数学课本）。

$$\cos 0=1. \tag{12}$$

$$\sin(2n\pi+\alpha)=\sin\alpha \quad (n=\pm 1,\pm 2,\cdots). \tag{13}$$

$$\cos(2n\pi+\alpha)=\cos\alpha \quad (n=\pm 1,\pm 2,\cdots). \tag{14}$$

$$\sin(-\alpha)=-\sin\alpha=\sin(\pi+\alpha)=\cos\left(\frac{\pi}{2}+\alpha\right). \tag{15}$$

$$\cos(-\alpha)=\cos\alpha=\sin\left(\frac{\pi}{2}+\alpha\right). \tag{16}$$

$$\cos(\pi+\alpha)=-\cos\alpha=\sin\left(\frac{3\pi}{2}+\alpha\right). \tag{17}$$

$$\cos\left(\frac{3\pi}{2}+\alpha\right)=\sin\alpha. \tag{18}$$

$$\cos(\alpha+\beta)=\cos\alpha\cdot\cos\beta-\sin\alpha\cdot\sin\beta. \tag{19}$$

(13) 式（或 (14) 式）说明，从角α再多转2π的整数倍那样大的角时，正弦函数（或余弦函数）的值不变，这个性质叫作正弦函数（或余弦函数）的周期性，2π叫作它的周期.

利用正弦函数（或余弦函数）的周期性，求大于2π的任意角的正弦函数（或余弦函数）可以转化为求不小于 0 而小于2π的角的正弦函数值（或余弦函数值）.

由 (16) 式得到$\sin\frac{\pi}{2}=\cos 0$，故由(12)式有$\sin\frac{\pi}{2}=1$.

由 (12) 和 (17) 式有 $\sin\frac{3\pi}{2}=\cos\pi=-1$. 在 (19) 式中取 $\beta=-\alpha$, 则由 (12), (16) 和 (15) 式我们有

$$1=\cos 0=\cos\alpha\cdot\cos(-\alpha)-\sin\alpha\cdot\sin(-\alpha)$$
$$=\cos^2\alpha+\sin^2\alpha. \tag{20}$$

由 (12) 和 (20) 式我们有 $\sin 0=0$. 因而使用 (15) 和 (18) 式我们有

$$\sin\pi=\cos\frac{\pi}{2}=\cos\frac{3\pi}{2}=0.$$

由 (12), (13), (14) 式和 $\sin 0=0$ 我们有

$$\sin 2\pi=0,\quad \cos 2\pi=1,$$

故得到

$$\sin 0=0,\quad \sin\frac{\pi}{2}=1,\quad \sin\pi=0,\quad \sin\frac{3\pi}{2}=-1,$$
$$\sin 2\pi=0, \tag{21}$$
$$\cos 0=1,\quad \cos\frac{\pi}{2}=0,\quad \cos\pi=-1,\quad \cos\frac{3\pi}{2}=0,$$
$$\cos 2\pi=1. \tag{22}$$

由 (18), (19)和 (17) 式我们有

$$\sin(\alpha+\beta)=\cos\left(\frac{3\pi}{2}+\alpha+\beta\right)=\cos\left(\frac{3\pi}{2}+\alpha\right)\cos\beta$$
$$-\sin\left(\frac{3\pi}{2}+\alpha\right)\sin\beta=\sin\alpha\cdot\cos\beta+\cos\alpha\cdot\sin\beta. \tag{23}$$

当 α 是任一个实数时,我们将介绍一种方法,使用这个方法可以求出 $\sin\alpha$ 和 $\cos\alpha$ 的近似数值.

当 α_1 是一个实数时,我们可以求出一个整数 m 和一个实数 β_1, 使得 $\alpha_1=2m\pi+\beta_1$ 成立,其中 $-\frac{\pi}{4}\leqslant\beta_1\leqslant\frac{7\pi}{4}$. 由

(13) 和 (14) 式我们有

$$\sin\alpha_1 = \sin(2m\pi + \beta_1) = \sin\beta_1,$$
$$\cos\alpha_1 = \cos(2m\pi + \beta_1) = \cos\beta_1.$$

(I) 当 $\frac{\pi}{4} < \beta_1 \leqslant \frac{3\pi}{4}$ 时，在 (15) 和 (16) 式中取 $\alpha = \beta_1 - \frac{\pi}{2}$，这时我们有

$$\sin\beta_1 = \sin\left(\frac{\pi}{2} + \beta_1 - \frac{\pi}{2}\right) = \cos\left(\beta_1 - \frac{\pi}{2}\right),$$
$$\cos\beta_1 = \cos\left(\frac{\pi}{2} + \beta_1 - \frac{\pi}{2}\right) = \sin\left(-\left(\beta_1 - \frac{\pi}{2}\right)\right)$$
$$= \sin\left(\frac{\pi}{2} - \beta_1\right).$$

由于

$$\frac{\pi}{4} < \beta_1 \leqslant \frac{3\pi}{4},$$

得到

$$0 \leqslant \left|\beta_1 - \frac{\pi}{2}\right| \leqslant \frac{\pi}{4}.$$

(II) 当 $\frac{3\pi}{4} < \beta_1 \leqslant \frac{5\pi}{4}$ 时，在 (15) 和 (17) 式中取 $\alpha = \beta_1 - \pi$，这时我们有

$$\sin\beta_1 = \sin(\pi + \beta_1 - \pi) = \sin(\pi - \beta_1),$$
$$\cos\beta_1 = \cos(\pi + \beta_1 - \pi) = -\cos(\beta_1 - \pi).$$

由于

$$\frac{3\pi}{4} < \beta_1 \leqslant \frac{5\pi}{4},$$

得到

$$0 \leqslant |\beta_1 - \pi| \leqslant \frac{\pi}{4}.$$

(III) 当 $\frac{5\pi}{4} < \beta_1 \leqslant \frac{7\pi}{4}$ 时，在(17)和(18)式中取 $\alpha = \beta_1 - \frac{3\pi}{2}$，这时我们有

$$\sin\beta_1 = \sin\left(\frac{3\pi}{2} + \beta_1 - \frac{3\pi}{2}\right) = -\cos\left(\beta_1 - \frac{3\pi}{2}\right),$$

$$\cos\beta_1 = \cos\left(\frac{3\pi}{2} + \beta_1 - \frac{3\pi}{2}\right) = \sin\left(\beta_1 - \frac{3\pi}{2}\right).$$

由于

$$\frac{5\pi}{4} < \beta_1 \leqslant \frac{7\pi}{4},$$

得到

$$0 \leqslant \left|\beta_1 - \frac{3\pi}{2}\right| \leqslant \frac{\pi}{4}.$$

由于 $\sin(-\alpha) = -\sin\alpha$，$\cos(-\alpha) = \cos\alpha$ 和上述的(I)，(II)，(III)三种情形，我们知道如果想求任一个实数 α_1 的 $\sin\alpha_1$ 和 $\cos\alpha_1$ 的数值，可以化成为求 $\sin\beta$ 和 $\cos\beta$ 有关的问题，其中 $0 \leqslant \beta \leqslant \frac{\pi}{4}$. 令 $0! = 1$，又令 $1! = 1$，$2! = 1\times2=2$，$3! = 1\times2\times3 = 6$，而当 $n \geqslant 4$ 时则令 $n! = 1\times2\times3\times\cdots\times n$. 在实践中我们发现当 $0 \leqslant x \leqslant 0.12$ 时，可用

$$\sum_{n=0}^{1}\frac{(-1)^n x^{2n+1}}{(2n+1)!}\left(\text{即 } x - \frac{x^3}{6}\right) \text{来近似} \sin x.$$

当 $0.12 < x \leqslant 0.4$ 时，可用

$$\sum_{n=0}^{2}\frac{(-1)^n x^{2n+1}}{(2n+1)!}\left(\text{即 } x - \frac{x^3}{6} + \frac{x^5}{120}\right) \text{来近似} \sin x.$$

当 $0.4 < x \leqslant \frac{\pi}{4}$ 时，可用

$$\sum_{n=0}^{3}\frac{(-1)^n x^{2n+1}}{(2n+1)!}\left(即\ x-\frac{x^3}{6}+\frac{x^5}{120}-\frac{x^7}{5040}\right)来近似 \sin x.$$

使用这些方法来近似 $\sin x$，我们至少可保证在小数点后的前六位数字都是准确的。 在实践中我们发现当 $0\leqslant x\leqslant 0.04$ 时，可用

$$\sum_{n=0}^{1}\frac{(-1)^n x^{2n}}{(2n)!}\left(即\ 1-\frac{x^2}{2}\right)来近似 \cos x.$$

当 $0.04<x\leqslant 0.16$ 时，可用

$$\sum_{n=0}^{2}\frac{(-1)^n x^{2n}}{(2n)!}\left(即\ 1-\frac{x^2}{2}+\frac{x^4}{24}\right)来近似 \cos x.$$

当 $0.16<x\leqslant 0.5$ 时，可用

$$\sum_{n=0}^{3}\frac{(-1)^n x^{2n}}{(2n)!}\left(即\ 1-\frac{x^2}{2}+\frac{x^4}{24}-\frac{x^6}{720}\right)来近似 \cos x.$$

当 $0.5<x\leqslant\frac{\pi}{4}\leqslant 0.786$ 时，可用

$$\sum_{n=0}^{4}\frac{(-1)^n x^{2n}}{(2n)!}\left(即\ 1-\frac{x^2}{2}+\frac{x^4}{24}-\frac{x^6}{720}+\frac{x^8}{40320}\right)来近似$$

$\cos x$。使用这些方法来近似 $\cos x$，我们至少可保证在小数点后的前六位数字是准确的。

例如

$$\sin 0.12=0.119712207\cdots,$$

可是

$$0.12-\frac{(0.12)^3}{6}=0.119712.$$

$$\sin 0.4=0.389418342\cdots,$$

可是

$$0.4-\frac{(0.4)^3}{6}+\frac{(0.4)^5}{120}=0.3894186\cdots.$$

$$\sin\frac{\pi}{4}=0.707106781\cdots,$$

可是

$$\frac{\pi}{4}-\frac{\pi^3}{6\times 4^3}+\frac{\pi^5}{120\times 4^5}-\frac{\pi^7}{5040\times 4^7}$$
$$=0.7071064\cdots.$$

$$\cos 0.04=0.999200106\cdots,$$

可是

$$1-\frac{(0.04)^2}{2}=0.9992.$$

$$\cos 0.16=0.987227283\cdots,$$

可是

$$1-\frac{(0.16)^2}{2}+\frac{(0.16)^4}{24}=0.9872273\cdots.$$

$$\cos 0.5=0.87758256\cdots,$$

可是

$$1-\frac{(0.5)^2}{2}+\frac{(0.5)^4}{24}-\frac{(0.5)^6}{720}=0.8775824\cdots.$$

$$\cos\frac{\pi}{4}=0.707106781\cdots,$$

可是

$$1-\frac{\pi^2}{2\times 4^2}+\frac{\pi^4}{24\times 4^4}-\frac{\pi^6}{720\times 4^6}$$
$$+\frac{\pi^8}{40320\times 4^8}=0.7071068\cdots.$$

我们现在使用这种方法来求sin 90。
由于

$$90=28\pi+2.0354056\cdots,$$

故由(I)有

$$\sin 90 = \cos\left(2.0354056\cdots - \frac{\pi}{2}\right) = \cos 0.464609\cdots,$$

故可用

$$\sum_{n=0}^{3}\frac{(-1)^n(0.464609)^{2n}}{(2n)!} \simeq \sin 90.$$

由于

$$1 - \frac{(0.464609)^2}{2} + \frac{(0.464609)^4}{24} - \frac{(0.464609)^6}{720}$$

$$\simeq 0.89399,$$

故得到

$$\sin 90 \simeq 0.89399.$$

§3. 复数的指数式

如果我们定义

$$e^{i\theta} = \cos\theta + i\sin\theta, \qquad (24)$$

其中 θ 是一个实数，那么复数 $z = r(\cos\theta + i\sin\theta)$ 就可以表示为简单形式

$$z = re^{i\theta}.$$

其中 r 是一个实数，而 $z = re^{i\theta}$ 称为复数的指数式.

达里，$e^{i\theta}$ 是作为一个记号引进来的，它代表复数 $\cos\theta + i\sin\theta$. 由 (21) 和 (22) 式我们有

$$e^{i0} = \cos 0 + i\sin 0 = 1, \quad e^{i\frac{\pi}{2}} = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2} = i, \qquad (25)$$

$$e^{i\pi} = \cos\pi + i\sin\pi = -1, \; e^{i\frac{3\pi}{2}} = \cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2} = -i. \qquad (26)$$

设 n 是一个整数而 θ 是一个实数，则由 (13) 和 (14) 式我们有

$$e^{i(2\pi n+\theta)} = \cos(2\pi n + \theta) + i\sin(2\pi n + \theta)$$
$$= \cos\theta + i\sin\theta = e^{i\theta}. \qquad (27)$$

由 (20) 式我们知道 $e^{i\theta}$ 的绝对值等于 1，即

$$|e^{i\theta}| = \sqrt{\cos^2\theta + \sin^2\theta} = 1. \tag{28}$$

引理 1 设 θ_1 和 θ_2 是二个实数，则我们有

$$e^{i(\theta_1+\theta_2)} = e^{i\theta_1} \cdot e^{i\theta_2}.$$

证 由 (24) 式我们有

$$\begin{aligned} e^{i\theta_1} \cdot e^{i\theta_2} &= (\cos\theta_1 + i\sin\theta_1)(\cos\theta_2 + i\sin\theta_2) \\ &= \cos\theta_1 \cdot \cos\theta_2 + i^2\sin\theta_1 \cdot \sin\theta_2 + i\sin\theta_1 \\ &\quad \cdot \cos\theta_2 + i\cos\theta_1 \cdot \sin\theta_2 \\ &= \cos\theta_1 \cdot \cos\theta_2 - \sin\theta_1 \cdot \sin\theta_2 \\ &\quad + i(\sin\theta_1 \cdot \cos\theta_2 + \cos\theta_1 \cdot \sin\theta_2). \end{aligned}$$

故由 (19) 和 (23) 式我们有

$$e^{i\theta_1} \cdot e^{i\theta_2} = \cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2). \tag{29}$$

由 (24) 式我们有

$$e^{i(\theta_1+\theta_2)} = \cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2). \tag{30}$$

由 (29) 式和 (30) 式知道引理 1 成立.

定义 3 设 n 是一个非负整数而 $z = a + bi$，其中 a，b 都是实数.令 $z^0 = 1$，$z^1 = z$，当 $n \geqslant 2$ 时我们说复数 z 的 n 次方就是 n 个 z 的连乘而成的，即

$$z^n = \underbrace{z \cdot z \cdots z}_{n\text{个}}.$$

引理 2 设 n 是一个正整数，θ 是一个实数，则我们有

$$(e^{i\theta})^n = e^{in\theta}.$$

证 当 $n = 1$ 时由 $(e^{i\theta})^1 = e^{i\theta}$，故本引理成立．现在设 $k \geqslant 2$，而当 n 等于 $1, 2, \cdots, k-1$ 时本引理都成立，则由引理 1 我们有

$$(e^{i\theta})^k = (e^{i\theta})^{k-1} \cdot e^{i\theta} = e^{i(k-1)\theta} \cdot e^{i\theta} = e^{ik\theta}.$$

故当 $n = k$ 时本引理也成立，而由数学归纳法知道引理 2 成立.

例 7 设

$$\sin\alpha+\sin\beta+\sin\gamma=\cos\alpha+\cos\beta+\cos\gamma=0,$$

请证明

$$3e^{i(\alpha+\beta+\gamma)}=e^{3i\alpha}+e^{3i\beta}+e^{3i\gamma}$$

成立. 因而有

$$3\cos(\alpha+\beta+\gamma)=\cos 3\alpha+\cos 3\beta+\cos 3\gamma,$$

$$3\sin(\alpha+\beta+\gamma)=\sin 3\alpha+\sin 3\beta+\sin 3\gamma.$$

证 我们有

$$\begin{aligned}(a+b+c)&(a^2+b^2+c^2-ab-bc-ca)\\ &=a^3+ab^2+ac^2-a^2b-abc-ca^2+ba^2+b^3\\ &\quad+bc^2-ab^2-b^2c-bca+ca^2+cb^2+c^3\\ &\quad-abc-bc^2-c^2a\\ &=a^3+b^3+c^3+ba^2-a^2b-ca^2+ca^2+ab^2\\ &\quad-ab^2+ac^2-c^2a+bc^2-bc^2-b^2c+cb^2-3abc\\ &=a^3+b^3+c^3-3abc.\end{aligned}\qquad(31)$$

我们令

$$a=e^{i\alpha},\quad b=e^{i\beta},\quad c=e^{i\gamma}.$$

由于假设

$$\sin\alpha+\sin\beta+\sin\gamma=\cos\alpha+\cos\beta+\cos\gamma=0,$$

故得到

$$\begin{aligned}a+b+c=e^{i\alpha}+e^{i\beta}+e^{i\gamma}&=\cos\alpha+i\sin\alpha+\cos\beta\\ &\quad+i\sin\beta+\cos\gamma+i\sin\gamma=0.\end{aligned}\qquad(32)$$

由 (31) 和 (32) 式得到

$$(e^{i\alpha})^3+(e^{i\beta})^3+(e^{i\gamma})^3=3e^{i\alpha}\cdot e^{i\beta}\cdot e^{i\gamma}.$$

由引理 1 和引理 2 即得到

$$3e^{i(\alpha+\beta+\gamma)}=e^{3i\alpha}+e^{3i\beta}+e^{3i\gamma}.$$

故例 7 得证.

例 8 证明 $(\sin x+i\cos x)^n=e^{in(\frac{\pi}{2}-x)}$.

证 由引理 1 和 (25) 式我们有

$$e^{in(\frac{\pi}{2}-x)}=e^{in\frac{\pi}{2}}\cdot e^{-inx}=(e^{i\frac{\pi}{2}})^n e^{-inx}=(ie^{-ix})^n$$
$$=(i\cos x+i^2\sin(-x))^n=(\sin x+i\cos x)^n,$$

故例 8 得证。

例 9 证明恒等式

$$\sin(\alpha-\beta)\sin(\gamma-\delta)=\sin(\alpha-\delta)\sin(\gamma-\beta)$$
$$+\sin(\alpha-\gamma)\sin(\beta-\delta).$$

证 由于

$$(a^2-d^2)(c^2-b^2)+(a^2-c^2)(b^2-d^2)$$
$$=a^2c^2-a^2b^2-c^2d^2+b^2d^2+a^2b^2-a^2d^2$$
$$-b^2c^2+c^2d^2$$
$$=a^2c^2-a^2d^2+b^2d^2-b^2c^2$$
$$=(a^2-b^2)(c^2-d^2), \tag{33}$$

令 $a=e^{i\alpha},\quad b=e^{i\beta},\quad c=e^{i\gamma},\quad d=e^{i\delta},$

则我们有

$$(a^2-b^2)(c^2-d^2)=(e^{2i\alpha}-e^{2i\beta})(e^{2i\gamma}-e^{2i\delta})$$
$$=e^{i(\alpha+\beta)}\cdot(e^{i(\alpha-\beta)}-e^{-i(\alpha-\beta)})\cdot e^{i(\gamma+\delta)}\cdot(e^{i(\gamma-\delta)}-e^{-i(\gamma-\delta)})$$
$$=e^{i(\alpha+\beta+\gamma+\delta)}(\cos(\alpha-\beta)+i\sin(\alpha-\beta)$$
$$-\cos(-(\alpha-\beta))-i\sin(-(\alpha-\beta)))$$
$$\times(\cos(\gamma-\delta)+i\sin(\gamma-\delta)-\cos(-(\gamma-\delta))$$
$$-i\sin(-(\gamma-\delta)))$$
$$=e^{i(\alpha+\beta+\gamma+\delta)}(2i\sin(\alpha-\beta))(2i\sin(\gamma-\delta))$$
$$=-4e^{i(\alpha+\beta+\gamma+\delta)}\sin(\alpha-\beta)\sin(\gamma-\delta). \tag{34}$$

$$(a^2-d^2)(c^2-b^2)=(e^{2i\alpha}-e^{2i\delta})(e^{2i\gamma}-e^{2i\beta})$$
$$=e^{i(\alpha+\delta)}(e^{i(\alpha-\delta)}-e^{-i(\alpha-\delta)})e^{i(\gamma+\beta)}(e^{i(\gamma-\beta)}-e^{-i(\gamma-\beta)})$$
$$=-4e^{i(\alpha+\delta+\gamma+\beta)}\sin(\alpha-\delta)\sin(\gamma-\beta). \tag{35}$$

$$(a^2-c^2)(b^2-d^2)=(e^{2i\alpha}-e^{2i\gamma})(e^{2i\beta}-e^{2i\delta})$$
$$=e^{i(\alpha+\gamma)}(e^{i(\alpha-\gamma)}-e^{-i(\alpha-\gamma)})e^{i(\beta+\delta)}(e^{i(\beta-\delta)}-e^{-i(\beta-\delta)})$$

$$= -4e^{i(\alpha+\beta+\gamma+\delta)}\sin(\alpha-\gamma)\cdot\sin(\beta-\delta). \qquad (36)$$

由(33)到(36)式我们有

$$-4e^{i(\alpha+\beta+\gamma+\delta)}\sin(\alpha-\beta)\sin(\gamma-\delta)$$
$$= -4e^{i(\alpha+\beta+\gamma+\delta)}\sin(\alpha-\delta)\sin(\gamma-\beta)$$
$$-4e^{i(\alpha+\beta+\gamma+\delta)}\sin(\alpha-\gamma)\sin(\beta-\delta).$$

由于 $e^{i(\alpha+\beta+\gamma+\delta)}\neq 0$，可将 $-4e^{i(\alpha+\beta+\gamma+\delta)}$ 同时除以上式中的两边，则例 9 得证.

引理 3 设 n 是一个正整数而 $z=a+bi$ 是一个复数，则当 $z\neq 1$ 时我们有

$$\sum_{m=0}^{n} z^m = \frac{1-z^{n+1}}{1-z}.$$

证 当 $n=1$ 时我们有

$$1+z=\frac{(1+z)(1-z)}{1-z}=\frac{1-z^2}{1-z},$$

故当 $n=1$ 时本引理成立. 现设 $k\geqslant 2$，而当 n 等于 $1,2,\cdots,k-1$ 时本引理都成立，则我们有

$$\sum_{m=0}^{k} z^m=\sum_{m=0}^{k-1} z^m+z^k=\frac{1-z^k}{1-z}+z^k=\frac{1-z^{k+1}}{1-z}.$$

故当 $n=k$ 时本引理也成立，而由数学归纳法知道引理 3 成立.

引理 4 我们有

$$\sum_{m=0}^{n-1} e^{i(\theta+m\varphi)}=e^{i\left(\theta+\frac{n-1}{2}\varphi\right)}\cdot\frac{\sin\frac{n\varphi}{2}}{\sin\frac{\varphi}{2}},$$

其中 n 是一个正整数，$\varphi\neq 2l\pi$，其中 l 是任一个整数，即 $\left\{\frac{\varphi}{2\pi}\right\}\neq 0$（$\{x\}$表示 $x-[x]$，见第七章的定义 3）.

证 由于 $\left\{\dfrac{\varphi}{2\pi}\right\}\neq 0$，故有 $e^{i\varphi}\neq 1$. 由引理 3，我们有

$$\sum_{m=0}^{n-1} e^{im\varphi}=\frac{1-e^{in\varphi}}{1-e^{i\varphi}}=\frac{e^{\frac{in\varphi}{2}}\left(e^{\frac{in\varphi}{2}}-e^{-\frac{in\varphi}{2}}\right)}{e^{\frac{i\varphi}{2}}\left(e^{\frac{i\varphi}{2}}-e^{-\frac{i\varphi}{2}}\right)}=e^{i\frac{n\varphi}{2}-\frac{i\varphi}{2}}$$

$$\times\frac{\cos\frac{n\varphi}{2}+i\sin\frac{n\varphi}{2}-\cos\left(-\frac{n\varphi}{2}\right)-i\sin\left(-\frac{n\varphi}{2}\right)}{\cos\frac{\varphi}{2}+i\sin\frac{\varphi}{2}-\cos\left(-\frac{\varphi}{2}\right)-i\sin\left(-\frac{\varphi}{2}\right)}$$

$$=e^{i\frac{n-1}{2}\varphi}\cdot\frac{\sin\frac{n\varphi}{2}}{\sin\frac{\varphi}{2}}.$$

将上式两边同时乘以 $e^{i\theta}$，则本引理得证.

例 10 设 n 是一个正整数而 $\left\{\dfrac{\varphi}{2\pi}\right\}\neq 0$，则我们有

$$\sum_{m=0}^{n-1}\cos(\theta+m\varphi)=\frac{\sin\frac{n\varphi}{2}}{\sin\frac{\varphi}{2}}\cdot\cos\left(\theta+\frac{n-1}{2}\varphi\right),\quad(37)$$

$$\sum_{m=0}^{n-1}\sin(\theta+m\varphi)=\frac{\sin\frac{n\varphi}{2}}{\sin\frac{\varphi}{2}}\cdot\sin\left(\theta+\frac{n-1}{2}\varphi\right).\quad(38)$$

证 由引理 4 我们有

$$\sum_{m=0}^{n-1}\cos(\theta+m\varphi)+i\sum_{m=0}^{n-1}\sin(\theta+m\varphi)$$

$$=\frac{\sin\frac{n\varphi}{2}}{\sin\frac{\varphi}{2}}\cdot\cos\left(\theta+\frac{n-1}{2}\varphi\right)$$

$$+i\frac{\sin\frac{n\varphi}{2}}{\sin\frac{\varphi}{2}}\cdot\sin\left(\theta+\frac{n-1}{2}\varphi\right),$$

即

$$\sum_{m=0}^{n-1}\cos(\theta+m\varphi)-\frac{\sin\frac{n\varphi}{2}}{\sin\frac{\varphi}{2}}\cdot\cos\left(\theta+\frac{n-1}{2}\varphi\right)$$

$$+i\left(\sum_{m=0}^{n-1}\sin(\theta+m\varphi)-\frac{\sin\frac{n\varphi}{2}}{\sin\frac{\varphi}{2}}\right.$$

$$\left.\times\sin\left(\theta+\frac{n-1}{2}\varphi\right)\right)=0.$$

故例 10 得证.

在例 10 中取 $\varphi=\theta$, 则当 $\left\{\frac{\theta}{2\pi}\right\}\neq 0$ 时我们有

$$\sum_{m=1}^{n}\cos m\theta=\frac{\sin\frac{n\theta}{2}}{\sin\frac{\theta}{2}}\cdot\cos\frac{(n+1)\theta}{2},\tag{39}$$

$$\sum_{m=1}^{n}\sin m\theta=\frac{\sin\frac{n\theta}{2}}{\sin\frac{\theta}{2}}\cdot\sin\frac{(n+1)\theta}{2}.\tag{40}$$

在例 10 中取 $\varphi=2\theta$, 则当 $\left\{\frac{\theta}{\pi}\right\}\neq 0$ 时我们有

$$\sum_{m=1}^{n}\cos(2m-1)\theta=\frac{\sin n\theta}{\sin\theta}\cdot\cos n\theta,\tag{41}$$

$$\sum_{m=1}^{n} \sin(2m-1)\theta = \frac{\sin^2 n\theta}{\sin\theta}. \tag{42}$$

§4. 三角和的概念

设m是一个$\geqslant 2$的整数而r是一个$0 \leqslant r \leqslant m-1$的整数. 由(24)式我们有

$$e^{2\pi i\frac{r}{m}} = \cos\frac{2\pi r}{m} + i\sin\frac{2\pi r}{m}.$$

由引理2、(27)和(25)式我们有

$$(e^{2\pi i\frac{r}{m}})^m = e^{2\pi ir} = 1,$$

故满足方程式 $z^m = 1$ 的复数z有m个,即

$$e^{2\pi i\frac{r}{m}},$$

其中 $r = 0, 1, \cdots, m-1$. 设a, b都是整数且满足同余式$a \equiv b \pmod m$, 故有 $a = b + mt$, 其中t是一个整数. 由引理1和(27)式我们有

$$e^{2\pi i\frac{a}{m}} = e^{2\pi it + 2\pi i\frac{b}{m}} = e^{2\pi it} \cdot e^{2\pi i\frac{b}{m}} = e^{2\pi i\frac{b}{m}}. \tag{43}$$

设a, b, c都是整数且满足同余式$a + b \equiv c \pmod m$, 则有$c = a + b + mt$, 其中t是一个整数. 由引理1和(27)式我们有

$$e^{2\pi i\frac{c}{m}} = e^{2\pi it + 2\pi i\frac{a+b}{m}} = e^{2\pi i\frac{a+b}{m}} = e^{2\pi i\frac{a}{m}} \cdot e^{2\pi i\frac{b}{m}}. \tag{44}$$

在计算三角和时, 常使用(43)和(44)式. 所谓三角和就是形如$\sum_x e^{2\pi if(x)}$的和,其中$f(x)$是实函数,而x通过预先指定的某些整数.本节只打算讨论几种简单三角和的基本性质.

引理5 设n是一个正整数而a是一个整数,则我们有

$$\sum_{m=0}^{n-1} e^{2\pi i\frac{am}{n}} = \begin{cases} n, & \text{当 } n \mid a \text{ 时}, \\ 0, & \text{当 } n \nmid a \text{ 时}. \end{cases}$$

因而当 $n \mid a$ 时我们有

$$\sum_{m=0}^{n-1} \cos \frac{2\pi am}{n} = n, \quad \sum_{m=0}^{n-1} \sin \frac{2\pi am}{n} = 0.$$

当 $n \nmid a$ 时则有

$$\sum_{m=0}^{n-1} \cos \frac{2\pi am}{n} = \sum_{m=0}^{n-1} \sin \frac{2\pi am}{n} = 0.$$

证 当 $n \mid a$ 时，由(27)和(25)式有 $e^{2\pi i \frac{am}{n}} = 1$，因而

$$\sum_{m=0}^{n-1} e^{2\pi i \frac{am}{n}} = n.$$

当 $n \nmid a$ 时，则由(27)式知道 $e^{2\pi i \frac{a}{n}} \neq 1$，所以由引理 2 和引理 3 我们有

$$\sum_{m=0}^{n-1} e^{2\pi i \frac{am}{n}} = \sum_{m=0}^{n-1} (e^{2\pi i \frac{a}{n}})^m = \frac{1-(e^{2\pi i \frac{a}{n}})^n}{1-e^{2\pi i \frac{a}{n}}}$$

$$= \frac{1-e^{2\pi i a}}{1-e^{2\pi i \frac{a}{n}}} = 0.$$

引理 6 设 α 是任一个实数而 n 是一个正整数，则我们有

$$\left|\sum_{m=1}^{n} e^{2\pi i \alpha m}\right| \leqslant \min\left(n, \frac{1}{|\sin \pi\alpha|}\right),$$

其中 $\min\left(n, \frac{1}{|\sin \pi\alpha|}\right)$ 表示 n 和 $\frac{1}{|\sin \pi\alpha|}$ 两个数中较小的那一个.

证 假设 α 不是整数，则 $e^{2\pi i\alpha} \neq 1$，这时由引理 2 和引理 3 我们有

$$\sum_{m=1}^{n} e^{2\pi i \alpha m} = e^{2\pi i\alpha} \sum_{m=0}^{n-1} e^{2\pi i \alpha m} = e^{2\pi i\alpha} \sum_{m=0}^{n-1} (e^{2\pi i \alpha})^m$$

$$= \frac{e^{2\pi i\alpha}(1-e^{2\pi i n\alpha})}{1-e^{2\pi i\alpha}}. \tag{45}$$

由 (28) 式我们有

$$|e^{2\pi i\alpha}|=1,$$

由例 4 和 (28) 式我们有

$$|1-e^{2\pi in\alpha}|\leqslant 1+|e^{2\pi in\alpha}|=1+1=2,$$

又由例 3 和 (28) 式我们有

$$\begin{aligned}|1-e^{2\pi i\alpha}|&=|e^{\pi\alpha i}(e^{-\pi\alpha i}-e^{\pi\alpha i})|=|e^{-\pi\alpha i}-e^{\pi\alpha i}|\\&=|\cos(-\pi\alpha)+i\sin(-\pi\alpha)-\cos\pi\alpha-i\sin\pi\alpha|\\&=2|\sin\pi\alpha|,\end{aligned}$$

故由例 3 和 (45) 式我们有

$$\left|\sum_{m=1}^{n}e^{2\pi i\alpha m}\right|\leqslant\frac{|e^{2\pi i\alpha}||1-e^{2\pi i\alpha n}|}{|1-e^{2\pi i\alpha}|}\leqslant\frac{1}{|\sin\pi\alpha|}. \qquad (46)$$

由例 4 和 (28) 式我们有

$$\left|\sum_{m=1}^{n}e^{2\pi i\alpha m}\right|\leqslant\sum_{m=1}^{n}\left|e^{2\pi i\alpha m}\right|=n. \qquad (47)$$

由 (46) 和 (47) 式知道当 α 不是整数时，引理 6 成立；当 α 是一个整数时，则由于 $\sin\pi\alpha=0$，故引理 6 也成立.

引理 7 设 n 是一个 $\geqslant 2$ 的整数，则我们有

$$\sum_{k=1}^{n-1}ke^{2\pi i\frac{k}{n}}=\frac{n}{e^{2\pi i\frac{1}{n}}-1}.$$

证 当 $n=2$ 时，则由 (26) 式知道本引理成立. 现在设 $n\geqslant 3$，我们有

$$\begin{aligned}\left(\sum_{k=1}^{n-1}ke^{2\pi i\frac{k}{n}}\right)\left(e^{2\pi i\frac{1}{n}}-1\right)&=\sum_{k=1}^{n-1}ke^{2\pi i\frac{k+1}{n}}-\sum_{k=1}^{n-1}ke^{2\pi i\frac{k}{n}}\\&=(n-1)e^{2\pi i\frac{n}{n}}+\sum_{k=2}^{n-1}(k-1)e^{2\pi i\frac{k}{n}}-\sum_{k=1}^{n-1}ke^{2\pi i\frac{k}{n}}\\&=n-1-\sum_{k=1}^{n-1}e^{2\pi i\frac{k}{n}}=n-\sum_{k=0}^{n-1}e^{2\pi i\frac{k}{n}}.\end{aligned} \qquad (48)$$

由引理 5 我们有

$$\sum_{k=0}^{n-1} e^{2\pi i \frac{k}{n}} = 0,$$

故由

$$e^{2\pi i \frac{1}{n}} - 1 \neq 0$$

和 (48) 式知道引理 7 成立.

引理 8 设 n 是一个 > 2 的整数，则我们有

$$\sum_{m=1}^{n-1} m \cos \frac{2\pi m}{n} = -\frac{n}{2},$$

$$\sum_{m=1}^{n-1} m \sin \frac{2\pi m}{n} = -\frac{n\left(1 + \cos \frac{2\pi}{n}\right)}{2 \sin \frac{2\pi}{n}}.$$

证 我们有

$$\frac{1}{e^{2\pi i \frac{1}{n}} - 1} = \frac{e^{-2\pi i \frac{1}{n}} + 1}{(e^{2\pi i \frac{1}{n}} - 1)(e^{-2\pi i \frac{1}{n}} + 1)}$$

$$= \frac{1 + \cos\left(-\frac{2\pi}{n}\right) + i \sin\left(-\frac{2\pi}{n}\right)}{e^{2\pi i \frac{1}{n}} - e^{-2\pi i \frac{1}{n}}}$$

$$= \frac{1 + \cos \frac{2\pi}{n} - i \sin \frac{2\pi}{n}}{2i \sin \frac{2\pi}{n}}$$

$$= -\frac{1}{2} - \frac{1 + \cos \frac{2\pi}{n}}{2 \sin \frac{2\pi}{n}} i.$$

由引理 7 我们有

$$\sum_{m=1}^{n-1} m e^{2\pi i \frac{m}{n}} - \frac{n}{e^{2\pi i \frac{1}{n}} - 1} = 0$$

$$= \sum_{m=1}^{n-1} m\cos\frac{2\pi m}{n} + i\sum_{m=1}^{n-1} m\sin\frac{2\pi m}{n}$$

$$- n\left(-\frac{1}{2} - \left(\frac{1+\cos\frac{2\pi}{n}}{2\sin\frac{2\pi}{n}}\right)i\right)$$

$$= \sum_{m=1}^{n-1} m\cos\frac{2\pi m}{n} + \frac{n}{2} + \left(\sum_{m=1}^{n-1} m\sin\frac{2\pi m}{n}\right.$$

$$\left. + \frac{\left(1+\cos\frac{2\pi}{n}\right)n}{2\sin\frac{2\pi}{n}}\right)i = 0,$$ 故引理 8 得证。

引理 9 设 n 和 m 是二个正整数且 $(n, m) = 1$，这时我们把三角和 $S(n, m) = \sum_{x=0}^{m-1} e^{2\pi i \frac{nx^2}{m}}$ 叫作高斯 (Gauss) 和。设 $(n, m) = 1$，当 m 是奇数时，我们有

$$|S(n, m)| = \sqrt{m}. \tag{49}$$

设 $(n, m) = 1$，当 $m = 4k$ 时(其中 k 是一个正整数)，我们有

$$|S(n, m)| = \sqrt{2m}. \tag{50}$$

设 $(n, m) = 1$，当 $m = 4k + 2$ 时(其中 k 是一个非负整数)，我们有

$$S(n, m) = 0. \tag{51}$$

故当 $(n, m) = 1$，$2|m$ 但 $4\nmid m$ 时，我们有

$$\sum_{x=0}^{m-1} \cos\frac{2\pi nx^2}{m} = \sum_{x=0}^{m-1} \sin\frac{2\pi nx^2}{m} = 0. \tag{52}$$

证 由 (24)，(15) 和 (16) 式我们有

$$|S(n, m)|^2 = \left(\sum_{x=0}^{m-1} \cos \frac{2\pi n x^2}{m}\right)^2 + \left(\sum_{x=0}^{m-1} \sin \frac{2\pi n x^2}{m}\right)^2$$

$$= \left(\sum_{x=0}^{m-1} \cos \frac{2\pi n x^2}{m} + i \sum_{x=0}^{m-1} \sin \frac{2\pi n x^2}{m}\right)\left(\sum_{x=0}^{m-1} \cos \frac{2\pi n x^2}{m} - i \sum_{x=0}^{m-1} \sin \frac{2\pi n x^2}{m}\right)$$

$$= \left\{\sum_{x=0}^{m-1} \left(\cos \frac{2\pi n x^2}{m} + i \sin \frac{2\pi n x^2}{m}\right)\right\}$$

$$\times \left\{\sum_{x=0}^{m-1} \left(\cos \frac{-2\pi n x^2}{m} + i \sin \frac{-2\pi n x^2}{m}\right)\right\}$$

$$= \sum_{x=0}^{m-1} e^{2\pi i \frac{nx^2}{m}} \sum_{y=0}^{m-1} e^{-2\pi i \frac{ny^2}{m}}$$

$$= \sum_{y=0}^{m-1} e^{-2\pi i \frac{ny^2}{m}} \left(\sum_{x=0}^{y-1} e^{2\pi i \frac{nx^2}{m}} + \sum_{x=y}^{m-1} e^{2\pi i \frac{nx^2}{m}}\right). \tag{53}$$

由 (27) 式我们有

$$\sum_{x=m}^{m+y-1} e^{2\pi i \frac{nx^2}{m}} = \sum_{t=0}^{y-1} e^{2\pi i \frac{n(m+t)^2}{m}}$$

$$= \sum_{t=0}^{y-1} e^{2\pi i n(m+2t)} \cdot e^{2\pi i \frac{nt^2}{m}} = \sum_{t=0}^{y-1} e^{2\pi i \frac{nt^2}{m}}. \tag{54}$$

由 (53), (54) 和引理 1 我们有

$$|S(n, m)|^2 = \sum_{y=0}^{m-1} e^{-2\pi i \frac{ny^2}{m}} \left(\sum_{x=m}^{m+y-1} e^{2\pi i \frac{nx^2}{m}} + \sum_{x=y}^{m-1} e^{2\pi i \frac{nx^2}{m}}\right)$$

$$= \sum_{y=0}^{m-1} e^{-2\pi i \frac{ny^2}{m}} \sum_{x=y}^{m+y-1} e^{2\pi i \frac{nx^2}{m}}$$

$$= \sum_{y=0}^{m-1} e^{-2\pi i \frac{ny^2}{m}} \sum_{t=0}^{m-1} e^{2\pi i \frac{n(y+t)^2}{m}}$$

$$=\sum_{y=0}^{m-1}\sum_{t=0}^{m-1}e^{2\pi i\frac{n((y+t)^2-y^2)}{m}}=\sum_{y=0}^{m-1}\sum_{t=0}^{m-1}e^{2\pi i\frac{n(2yt+t^2)}{m}}$$

$$=\sum_{x=0}^{m-1}e^{2\pi i\frac{nx^2}{m}}\sum_{y=0}^{m-1}e^{2\pi i\frac{2nxy}{m}}. \tag{55}$$

由引理 5 我们有

$$\sum_{y=0}^{m-1}e^{2\pi i\frac{2nxy}{m}}=\begin{cases}m, & 当\ m\mid 2nx\ 时;\\ 0, & 当\ m\nmid 2nx\ 时.\end{cases} \tag{56}$$

当 x 是任一个不大于 $m-1$ 的正整数时，则有 $m\nmid x$. 当 $(n, m)=1$ 而 m 是奇数时，则 $m\nmid 2n$. 故当 m 是一个奇数，$(n, m)=1$ 而 x 是任一个不大于 $m-1$ 的正整数时，则有 $m\nmid 2nx$. 当 $(n, m)=1$ 而 m 是一个奇数时，则由(55)和(56)式我们有

$$|S(n, m)|^2=me^{2\pi i\frac{0}{m}}+\sum_{x=1}^{m-1}e^{2\pi i\frac{nx^2}{m}}\sum_{y=0}^{m-1}e^{2\pi i\frac{2nxy}{m}}=m. \tag{57}$$

故当 $(n, m)=1$ 而 m 是奇数时，(49) 式成立. 设 m 是一个偶数. 当 x 是任一个不大于 $m-1$ 又不等于 $\frac{m}{2}$ 的正整数时，有 $\frac{m}{2}\nmid x$ 即 $m\nmid 2x$. 故当 m 是一个偶数，$(n, m)=1$ 而 x 是任一个不大于 $m-1$ 又不等于 $\frac{m}{2}$ 的正整数时，则有 $m\nmid 2nx$. 故当 $(n,m)=1$ 而 m 是一个偶数时，由(55)和(56)式我们有

$$|S(n, m)|^2=me^{2\pi i\frac{0}{m}}+e^{2\pi i\frac{n\left(\frac{m}{2}\right)^2}{m}}\sum_{y=0}^{m-1}e^{2\pi i\frac{nmy}{m}}$$

$$+\sum_{x=1}^{\frac{m}{2}-1}e^{2\pi i\frac{nx^2}{m}}\sum_{y=0}^{m-1}e^{2\pi i\frac{2nxy}{m}}+\sum_{x=\frac{m}{2}+1}^{m-1}e^{2\pi i\frac{nx^2}{m}}\sum_{y=0}^{m-1}e^{2\pi i\frac{2nxy}{m}}$$

$$= m(1 + e^{\frac{\pi mni}{2}}). \tag{58}$$

当 $(n, m) = 1$ 而 $m = 4k$ 时（其中 k 是一个正整数），则由 (25), (27) 和 (58) 式我们有

$$|S(n, m)|^2 = m(1 + e^{2kn\pi i}) = 2m.$$

故(50)式得证．当 $(n, m) = 1$ 而 $m = 4k + 2$ 时（其中 k 是一个非负整数），则由 $(n, m) = 1$ 知道 n 是一个奇数．设 $n = 2l + 1$（其中 l 是一个非负整数），则我们有

$$mn = (4k + 2)(2l + 1) = 4(2kl + k + l) + 2.$$

故由 (58), (27), (25) 和 (26) 式我们有

$$|S(n, m)|^2 = m(1 + e^{2\pi i\cdot(2kl+k+l)+\pi i})$$
$$= m(1 + e^{\pi i}) = 0.$$

因而(51)式得证．由(51)式知道(52)式成立，故本引理得证．

当 $k \geqslant 3$ 时我们用 $f(x)$ 来表示一个整数系数的多项式，即

$$f(x) = a_k x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_0.$$

其中 $a_i (i = 0, 1, 2, \cdots, k)$ 都是整数．设 q 是一个 >1 的整数，则当 $(a_1, \cdots, a_k, q) = 1$ 时，我们令

$$S(q, f(x)) = \sum_{x=1}^{q} e^{\frac{2\pi i f(x)}{q}}.$$

引理 10 设 k 是一个 $\geqslant 3$ 的整数而 l 是一个 $1 < l \leqslant k$ 的整数，a_k 是一个正整数，p 是一个素数，则当 $(p, ka_k) = 1$ 时我们有

$$\sum_{x=0}^{p^l-1} e^{2\pi i\frac{a_k x^k}{p^l}} = p^{l-1}, \tag{59}$$

即

$$\sum_{x=0}^{p^l-1} \cos\frac{2\pi a_k x^k}{p^l} = p^{l-1}, \quad \sum_{x=0}^{p^l-1} \sin\frac{2\pi a_k x^k}{p^l} = 0. \tag{60}$$

证 设 $x = p^{l-1}u + v$. 当 u 经过 $0, 1, \cdots, p-1$ v 而经过 $0, 1, \cdots, p^{l-1}-1$ 时，x 恰好经过 $0, 1, 2, \cdots, p^l-1$. 由于 $l \geqslant 2$, $l + l - 2 \geqslant 2 + l - 2 = l$ 而得到

$$p^{2(l-1)} \equiv 0 \pmod{p^l}. \tag{61}$$

现在我们来证明对于任何一个正整数 n

$$(p^{l-1}u + v)^n \equiv np^{l-1}uv^{n-1} + v^n \pmod{p^l} \tag{62}$$

都成立. 显见当 $n = 1$ 时 (62) 式成立. 现在设 $m \geqslant 2$ 而当 $n = m - 1$ 时 (62) 式能够成立. 由于

$$(p^{l-1}u + v)^{m-1} \equiv (m-1)p^{l-1}uv^{m-2} + v^{m-1} \pmod{p^l},$$

我们有

$$(p^{l-1}u + v)^m \equiv (p^{l-1}u + v)((m-1)p^{l-1}uv^{m-2} + v^{m-1}) \pmod{p^l}. \tag{63}$$

我们又有

$$(p^{l-1}u + v)((m-1)p^{l-1}uv^{m-2} + v^{m-1}) = (m-1)u^2v^{m-2}p^{2(l-1)} + m(p^{l-1}u)v^{m-1} + v^m. \tag{64}$$

由 (63), (64) 和 (61) 式我们知道当 $n = m$ 时 (62) 也能够成立，而由数学归纳法知道 (62) 式成立. 由 (62) 式我们有

$$(p^{l-1}u + v)^k \equiv kp^{l-1}uv^{k-1} + v^k + m_1p^l, \tag{65}$$

其中 m_1 是一个整数. 由 (25), (27), (65) 式和引理 1 我们有

$$\begin{aligned}
\sum_{x=0}^{p^l-1} e^{2\pi i\frac{a_kx^k}{p^l}} &= \sum_{u=0}^{p-1}\sum_{v=0}^{p^{l-1}-1} e^{2\pi i\frac{a_k(p^{l-1}u+v)^k}{p^l}} \\
&= \sum_{u=0}^{p-1}\sum_{v=0}^{p^{l-1}-1} e^{2\pi i\frac{a_k(kp^{l-1}uv^{k-1}+v^k)}{p^l}} \\
&= \sum_{u=0}^{p-1}\sum_{v=0}^{p^{l-1}-1} e^{2\pi i\frac{ka_kuv^{k-1}}{p}} \cdot e^{2\pi i\frac{a_kv^k}{p^l}} \\
&= \sum_{v=0}^{p^{l-1}-1} e^{2\pi i\frac{a_kv^k}{p^l}} \sum_{u=0}^{p-1} e^{2\pi i\frac{ka_kuv^{k-1}}{p}}.
\end{aligned} \tag{66}$$

由于 $k\geqslant 3$，$(p,a_k k)=1$ 和引理 5 我们有

$$\sum_{u=0}^{p-1} e^{2\pi i\frac{ka_k uv^{k-1}}{p}}=\begin{cases}p, & 当\ p|v\ 时;\\ 0, & 当\ p\nmid v\ 时.\end{cases} \tag{67}$$

由于 $1<l\leqslant k$，故当 $p|v$ 时有 $e^{2\pi i\frac{a_k v^k}{p^l}}=1$. 由(67)式知道当 $p|v$ 时，我们有

$$e^{2\pi i\frac{a_k v^k}{p^l}}\sum_{u=0}^{p-1} e^{2\pi i\frac{ka_k uv^{k-1}}{p}}=p. \tag{68}$$

由 (67) 式知道当 $p\nmid v$ 时，我们有

$$e^{2\pi i\frac{a_k v^k}{p^l}}\sum_{u=0}^{p-1} e^{2\pi i\frac{ka_k uv^{k-1}}{p}}=0. \tag{69}$$

在 $0,1,\cdots,p^{l-1}-1$ 中是 p 的倍数的数是

$$0,\ p,\ 2p,\cdots,(p^{l-2}-1)p,$$

共计有 p^{l-2} 个，故由 (66)，(68) 和 (69) 式知道 (59) 式成立. 由 (59) 式知道 (60) 式成立，故本引理得证.

引理 11 设 k 是一个 $\geqslant 3$ 的整数而 l 是一个 $>k$ 的整数，a_k 是一个正整数，p 是一个素数，则当 $(p,a_k k)=1$ 时我们有

$$\sum_{x=0}^{p^l-1} e^{2\pi i\frac{a_k x^k}{p^l}}=p^{k-1}\sum_{y=0}^{p^{l-k}-1} e^{2\pi i\frac{a_k y^k}{p^{l-k}}}.$$

证 在 $0,1,2,\cdots,p^{l-1}-1$ 中是 p 的倍数的数有

$$0,\ p,\ 2p,\cdots,(p^{l-2}-1)p. \tag{70}$$

由于 $l>k\geqslant 3$，(66)，(67) 和 (70) 式我们有

$$\sum_{x=0}^{p^l-1} e^{2\pi i\frac{a_k x^k}{p^l}}=p\sum_{y=0}^{p^{l-2}-1} e^{2\pi i\frac{a_k (py)^k}{p^l}}=p\sum_{y=0}^{p^{l-2}-1} e^{2\pi i\frac{a_k y^k}{p^{l-k}}}$$

$$=p\sum_{m=0}^{p^{k-2}-1}\sum_{n=0}^{p^{l-k}-1} e^{2\pi i\frac{a_k (mp^{l-k}+n)^k}{p^{l-k}}}=p\sum_{m=0}^{p^{k-2}-1}\sum_{n=0}^{p^{l-k}-1} e^{2\pi i\frac{a_k n^k}{p^{l-k}}}$$

$$= p^{k-1}\sum_{n=0}^{p^{l-k}-1} e^{2\pi i \frac{a_k n^k}{p^{l-k}}}.$$

故本引理得证.

引理 12 设 k 是一个 $\geqslant 3$ 的整数，$l = km + r$，其中 m，r 都是非负整数且 $1 < r \leqslant k$. 又设 a_k 是一个正整数，p 是一个素数，则当 $(p, ka_k) = 1$ 时我们有

$$\sum_{x=0}^{p^l-1} e^{2\pi i \frac{a_k x^k}{p^l}} = p^{l-m-1}, \tag{71}$$

即

$$\sum_{x=0}^{p^l-1} \cos \frac{2\pi a_k x^k}{p^l} = p^{l-m-1}, \quad \sum_{x=0}^{p^l-1} \sin \frac{2\pi a_k x^k}{p^l} = 0. \tag{72}$$

证 当 $m = 0$ 时由引理 10 知道本引理成立. 现在设 $n \geqslant 1$，而当 $m = n - 1$ 时 (71) 式成立，即设

$$\sum_{x=0}^{p^{k(n-1)+r}-1} e^{2\pi i \frac{a_k x^k}{p^{k(n-1)+r}}} = p^{k(n-1)+r-n} \tag{73}$$

成立. 由于 $n \geqslant 1$，$1 < r \leqslant k$，引理 11 和 (73) 式我们有

$$\sum_{x=0}^{p^{kn+r}-1} e^{2\pi i \frac{a_k x^k}{p^{kn+r}}} = p^{k-1} \sum_{y=0}^{p^{kn+r-k}-1} e^{2\pi i \frac{a_k y^k}{p^{k(n-1)+r}}}$$

$$= p^{k-1+k(n-1)+r-n} = p^{kn+r-n-1}.$$

故 (71) 式当 $m = n$ 时也成立，而由数学归纳法知道 (71) 式成立，由 (71) 式知道 (72) 式成立，故本引理得证.

设 p 是一个素数而 $f(x)$ 是一个 k 次整数系数的多项式. 估计三角和 $\sum_{x=1}^{p} e^{2\pi i \frac{f(x)}{p}}$ 的既很精确又很一般的方法首先是由我的老师华罗庚教授得到的. 下面的 (74) 式是 A. Weil 所证明的. (75) 式见华罗庚的《数论导引》.

定理 1 设 k 是一个 $\geqslant 3$ 的整数. 令

$$f(x)=a_kx^k+a_{k-1}x^{k-1}+\cdots+a_1x+a_0,$$

其中 $a_i(i=0,1,2,\cdots,k)$ 都是整数. 当 p 是一个素数而 $(a_k,a_{k-1},\cdots,a_1,p)=1$ 时,我们有

$$\left|\sum_{x=1}^{p}e^{2\pi i\frac{f(x)}{p}}\right|\leqslant(k-1)p^{\frac{1}{2}}. \tag{74}$$

当 $p\nmid a$ 时,我们有

$$\left|\sum_{x=1}^{p}e^{2\pi i\frac{ax^k}{p}}\right|\leqslant(\delta-1)p^{\frac{1}{2}}, \tag{75}$$

这里 $\delta=(k,p-1)$.

由于这个定理的证明需要很高深的数学理论和较长的计算,所以在这里不给以数学证明.

引理 13 设 k 是一个 $\geqslant3$ 的整数, $l=km+1$, 其中 m 是一个非负整数. 又设 a 是一个正整数, p 是一个素数,则当 $(p,ka)=(p-1,k)=1$ 时,我们有

$$\sum_{x=0}^{p^l-1}e^{2\pi i\frac{ax^k}{p^l}}=0, \tag{76}$$

即

$$\sum_{x=0}^{p^l-1}\cos\frac{2\pi ax^k}{p^l}=\sum_{x=0}^{p^l-1}\sin\frac{2\pi ax^k}{p^l}=0. \tag{77}$$

证 当 $m=0$ 时(即 $l=1$ 时),由定理 1 知道(76)式成立. 现在设 $n\geqslant1$, 而当 $m=n-1$ 时(即 $l=k(n-1)+1$ 时),(76)式成立,即设

$$\sum_{x=0}^{p^{k(n-1)+1}-1}e^{2\pi i\frac{ax^k}{p^{k(n-1)+1}}}=0 \tag{78}$$

成立. 由于 $n\geqslant1$, 引理 11 和(78)式我们有

$$\sum_{x=0}^{p^{kn+1}-1}e^{2\pi i\frac{ax^k}{p^{kn+1}}}=p^{k-1}\sum_{x=0}^{p^{k(n-1)+1}-1}e^{2\pi i\frac{ax^k}{p^{k(n-1)+1}}}=0.$$

故 (76) 式当 $m=n$ 时(即 $l=kn+1$ 时)也成立，而由数学归纳法知道 (76) 式成立. 由 (76) 式知道 (77) 式成立，故本引理得证.

设 p 是一个素数，l, q 是正整数而 $f(x)$ 是一个 k 次多项式，估计三角和 $\sum_{x=1}^{p^l} e^{2\pi i \frac{f(x)}{p^l}}$ 和 $\sum_{x=1}^{q} e^{2\pi i \frac{f(x)}{q}}$ 的既非常精确又非常一般的方法首先是由我的老师华罗庚教授得到的. 在华罗庚教授指导之下，我们证明了下面二个定理.

定理 2 设 k 是一个 $\geqslant 3$ 的整数而 l 是一个正整数. 令

$$f(x)=a_k x^k+a_{k-1}x^{k-1}+\cdots+a_1 x+a_0,$$

其中 $a_i(i=0,1,2,\cdots,k)$ 都是整数. 当 p 是一个素数而 $(a_k, a_{k-1},\cdots, a_1, p)=1$ 时，我们有

$$\left|\sum_{x=1}^{p^l} e^{2\pi i \frac{f(x)}{p^l}}\right| \leqslant C_1(k)p^{l(1-\frac{1}{k})},$$

其中

$$C_1(k)=\begin{cases} 1, & \text{当 } p\geqslant (k-1)^{\frac{2k}{k-2}} \text{ 时;} \\ k^{2/k}, & \text{当 } (k-1)^{\frac{2k}{k-2}}>p\geqslant (k-1)^{\frac{k}{k-2}} \text{ 时;} \\ k^{3/k}, & \text{当 } (k-1)^{\frac{k}{k-2}}>p>k \text{ 时;} \\ (k-1)k^{3/k}, & \text{当 } p\leqslant k \text{ 时.} \end{cases}$$

定理 3 设 k 是一个 $\geqslant 3$ 的整数而 q 是一个正整数. 令

$$f(x)=a_k x^k+a_{k-1}x^{k-1}+\cdots+a_1 x+a_0,$$

其中 $a_i(i=0,1,2,\cdots,k)$ 都是整数. 当 $(a_k, a_{k-1},\cdots, a_1, q)=1$ 时，我们有

$$\left|\sum_{x=1}^{q} e^{2\pi i \frac{f(x)}{q}}\right| \leqslant C_2(k)q^{1-\frac{1}{k}},$$

其中

$$C_2(k)=\begin{cases} e^{4k}, & \text{当 } k\geqslant 10 \text{ 时;} \\ e^{C_3(k)k}, & \text{当 } 3\leqslant k\leqslant 9 \text{ 时.} \end{cases}$$

又 $C_3(3)=6.1$，$C_3(4)=5.5$，$C_3(5)=5$，$C_3(6)=4.7$，$C_3(7)=4.4$，$C_3(8)=4.2$，$C_3(9)=4.05$.

由于这二个定理的证明需要很高深的数学理论和较长的计算，所以在这里不给以数学证明.

在解析数论中的不少著名问题（例如华林（Waring）问题）都需要 $\sum_{x=1}^{q} e^{2\pi i \frac{f(x)}{q}}$ 的精确估计值．设 $F(x)$ 是 x 的实函数，形如

$$\sum_{p\leqslant N} e^{2\pi i F(p)}$$

的精确估计值（这里和式中的 p 系经过所有不超过 N 的素数）在解析数论中起着非常重要的作用．华罗庚教授在这方面有卓越的贡献和许多优秀成果．在解析数论的研究中需要大量三角和和 $L(s,\chi)$ 的估计，在这方面我国有光荣的历史，华罗庚教授、闵嗣鹤教授、柯召教授、越民义、王元、潘承洞、尹文霖、丁夏畦、吴方、潘承彪和陈景润等同志都在这方面做过不少工作.

习　　题

1. 求适合下列方程的 x 和 y:

(i) $-4x+8yi+7=2x-3yi+7i$.

(ii) $x+yi=\sqrt{a+bi}$.

2. 设 z_1 和 z_2 是任意二个复数，证明:

$$|z_1-z_2|\geqslant\left||z_1|-|z_2|\right|.$$

3. 求27的立方根.

4. 证明下列三角恒等式:

(i) $\sin 3\alpha=3\sin\alpha-4\sin^3\alpha$,

$\cos 3\alpha=4\cos^3\alpha-3\cos\alpha$.

(ii) $\sin 4\alpha=4\sin\alpha\cos^3\alpha-4\sin^3\alpha\cos\alpha$,

$\cos 4\alpha=\cos^4\alpha-6\sin^2\alpha\cos^2\alpha+\sin^4\alpha$.

(iii) $\cos^4\alpha=\dfrac{1}{8}(\cos 4\alpha+4\cos 2\alpha+3)$.

(iv) $\sin^3\alpha=-\dfrac{1}{4}(\sin 3\alpha-3\sin\alpha)$.

5. 证明

(i) $$\sum_{k=1}^{n}\sin^2 k\alpha=\frac{1}{4\sin\alpha}[(2n+1)\sin\alpha-\sin(2n+1)\alpha].$$

(ii) $$\sum_{k=1}^{n}\cos^3 k\alpha=\frac{1}{4}\left[\frac{3\sin\dfrac{n\alpha}{2}}{\sin\dfrac{\alpha}{2}}\cos\frac{(n+1)\alpha}{2}+\frac{\sin\dfrac{3n\alpha}{2}}{\sin\dfrac{3\alpha}{2}}\cos\frac{3(n+1)\alpha}{2}\right].$$

6. 证明：$\dfrac{1+\sin\theta+i\cos\theta}{1+\sin\theta-i\cos\theta}=\sin\theta+i\cos\theta$，

并由此推出

$$\left(1+\sin\frac{\pi}{5}+i\cos\frac{\pi}{5}\right)^5+i\left(1+\sin\frac{\pi}{5}-i\cos\frac{\pi}{5}\right)^5$$

$$=0.$$

7. 求和：

$$A_n=1+r\cos\theta+r^2\cos 2\theta+\cdots+r^{n-1}\cos(n-1)\theta,$$

$$B_n=r\sin\theta+r^2\sin 2\theta+\cdots+r^{n-1}\sin(n-1)\theta.$$

8. 证明：$\theta\neq m\pi$ 时（m 为整数），

$$\sum_{k=1}^{\infty}\cos^{k-1}\theta\cos k\theta=0.$$

9. 试证：当 $\alpha\neq\dfrac{k}{2}\pi$ 时（k 是整数），

$$\cos\alpha+\sin 3\alpha+\cos 5\alpha+\sin 7\alpha+\cdots+\sin(4n-1)\alpha$$

$$=\frac{\sin 2n\alpha}{\sin 2\alpha}(\cos 2n\alpha+\sin 2n\alpha)(\cos\alpha+\sin\alpha).$$

10. 证明：

$$\operatorname{tg} n\alpha=\frac{\sin\alpha+\sin 3\alpha+\cdots+\sin(2n-1)\alpha}{\cos\alpha+\cos 3\alpha+\cdots+\cos(2n-1)\alpha}.$$

11. 设 m 是整数，$m>0$，ξ 通过与 m 互素的剩余系，证明：

$$\mu(m)=\sum_{\xi}e^{2\pi i\frac{\xi}{m}}.$$

这里 $\mu(m)$ 是 Möbius 函数.

12. 设 $m>1$，$(2A,m)=1$，a 是任意整数.

证明：$\left|\sum_{x=0}^{m-1}e^{2\pi i\frac{Ax^2+ax}{m}}\right|=\sqrt{m}$.

13. 设 $S(n,m)=\sum_{x=0}^{m-1}e^{2\pi i\frac{nx^2}{m}}$，若 $(m,m')=1$，则有

$$S(n, mm') = S(nm', m)S(nm, m').$$

14. 设 $C_q(m) = \sum_h e^{2\pi i \frac{hm}{q}}$,

h 通过与模 q 互素的剩余系. 证明:

(i) 若 $(q, q') = 1$, 则有

$$C_{qq'}(m) = C_q(m)C_{q'}(m).$$

(ii) $C_q(m) = \sum_{d|q,\, d|m} u\left(\frac{q}{d}\right)d.$

(等式右边表示对 q 和 m 的所有公因数求和.)

习 题 解 答

第五章

1. 证：由于 x_1，x_2 分别通过 m_1，m_2 个整数，因此 $m_2x_1+m_1x_2$ 正好通过 m_1m_2 个整数．由引理 5，若能证明这 m_1m_2 个整数对模 m_1m_2 互不同余，则这 m_1m_2 个整数是模 m_1m_2 的一个完全剩余系．

假定

$$m_2x_1'+m_1x_2'\equiv m_2x_1''+m_1x_2''\ (\text{mod}\ m_1m_1).$$

这里 x_1'，x_1'' 是 x_1 通过的模 m_1 的完全剩余系中的整数，而 x_2'，x_2'' 是 x_2 通过的模 m_2 的完全剩余系中的整数．所以

$$(m_2x_1'+m_1x_2')-(m_2x_1''+m_1x_2'')=m_1m_2q,\quad q\ \text{是整数}.$$

即

$$m_2(x_1'-x_1'')=m_1m_2q-m_1(x_2'-x_2'').$$

上式等号右边是 m_1 的倍数，因此 $m_1\mid m_2(x_1'-x_1'')$．又已知 $(m_1, m_2)=1$，所以 $m_1\mid(x_1'-x_1'')$．即

$$x_1'\equiv x_1''\ (\text{mod}\ m_1).$$

但 x_1'，x_1'' 是模 m_1 的一个完全剩余系中的数，由上式及引理 4 可知 $x_1'=x_1''$．用同样的方法可以证明 $x_2'=x_2''$．这说明 $m_2x_1+m_1x_2$ 所通过的 m_1m_2 个数对模 m_1m_2 互不同余．

2. 证：$k=2$ 的情形已由第 1 题予以证明．这里假定 $k>2$．显然 $M_1x_1+M_2x_2+\cdots+M_kx_k$ 正好通过 $m_1m_2\cdots m_k$ 个整数，由引理 5，只需证明这 $m_1m_2\cdots m_k$ 个整数对模 $m_1m_2\cdots m_k$ 两两不同余就够了．

假定

$$M_1x_1' + M_2x_2' + \cdots + M_kx_k' \equiv M_1x_1'' + M_2x_2'' + \cdots + M_kx_k'' \pmod{m_1m_2\cdots m_k}.$$

这里x_i'，x_i''是x_i通过模m_i的完全剩余系中的整数，$1\leqslant i\leqslant k$. 所以

$$M_1(x_1' - x_1'') \equiv M_2(x_2'' - x_2') + \cdots + M_k(x_k'' - x_k') \times \pmod{m_1m_2\cdots m_k}.$$

由于M_2，M_3，$\cdots$，M_k都能被m_1整除，因而上同余式的右边和模都能被m_1整除，所以

$$m_1 \mid M_1(x_1' - x_1'').$$

而$M_1 = m_2m_3\cdots m_k$，显然$(M_1, m_1) = 1$，所以$m_1 \mid (x_1' - x_1'')$. 又x_1'，x_1''是模m_1的一个完全剩余系中的数，由引理4可知$x_1' = x_1''$. 同样的方法可得$x_2' = x_2''$，$\cdots$，$x_k' = x_k''$. 这说明$M_1x_1 + M_2x_2 + \cdots + M_kx_k$所通过的$m_1m_2\cdots m_k$个整数对模$m_1m_2\cdots m_k$两两不同余.

3. 证：显然$x_1 + m_1x_2 + m_1m_2x_3 + \cdots + m_1m_2\cdots m_{k-1}x_k$正好通过$m_1m_2\cdots m_k$个整数，因而只需证明这些整数对模$m_1m_2\cdots m_k$两两不同余.

假定

$$x_1' + m_1x_2' + m_1m_2x_3' + \cdots + m_1m_2\cdots m_{k-1}x_k' \equiv x_1'' + m_1x_2'' + m_1m_2x_3'' + \cdots + m_1m_2\cdots m_{k-1}x_k'' \times \pmod{m_1m_2\cdots m_k}.$$

这里x_i'，x_i''是x_i通过的模m_i的完全剩余系中的整数，$1\leqslant i\leqslant k$. 因此

$$x_1' - x_1'' \equiv m_1q_1 \pmod{m_1m_2\cdots m_k}，\ q_1 \text{是整数}.$$

同余式的右边与模都能被m_1整除，所以$m_1 \mid (x_1' - x_1'')$，即$x_1' \equiv x_1'' \pmod{m_1}$. 但$x_1'$，$x_1''$是模$m_1$的一个完全剩余系中的整数，所以$x_1' = x_1''$.

这样就有同余式

$$m_1x_2' + m_1m_2x_3' + \cdots + m_1m_2\cdots m_{k-1}x_k'$$
$$\equiv m_1x_2'' + m_1m_2x_3'' + \cdots + m_1m_2\cdots m_{k-1}x_k''$$
$$\times \pmod{m_1m_2\cdots m_k}.$$

于是有

$$m_1(x_2' - x_2'') \equiv m_1m_2q_2 \pmod{m_1m_2\cdots m_k},\ q_2\text{是整数}.$$

也就是

$$x_2' - x_2'' \equiv m_2q_2 \pmod{m_2m_3\cdots m_k}.$$

同余式的右边与模都能被 m_2 整除，所以 $m_2|(x_2' - x_2'')$，即 $x_2' \equiv x_2'' \pmod{m_2}$，但 x_2'，x_2'' 是模 m_2 的一个完全剩余系中的整数，所以 $x_2' = x_2''$.

依此类推，可得 $x_3' = x_3'', \cdots, x_{k-1}' = x_{k-1}''$. 最后得

$$m_1m_2\cdots m_{k-1}x_k' \equiv m_1m_2\cdots m_{k-1}x_k'' \pmod{m_1m_2\cdots m_k}.$$

因而

$$x_k' \equiv x_k'' \pmod{m_k}.$$

由于 x_k'，x_k'' 是模 m_k 的一个完全剩余系中的整数，所以 $x_k' = x_k''$. 因而证明了 $x_1 + m_1x_2 + m_1m_2x_3 + \cdots + m_1m_2\cdots m_{k-1}x_k$ 通过模 $m_1m_2\cdots m_k$ 的完全剩余系.

4. (i) 证：若 N 不含有奇素因子，则由于 $N > 2$，因此 $N = 2^\alpha$，$\alpha \geqslant 2$. 由引理 14 得 $\varphi(N) = 2^{\alpha-1}$，$\alpha \geqslant 2$，因而 $2|\varphi(N)$.

若 N 含有奇素因子，设 p 是 N 的一个奇素因子，由引理 14 可知 $(p-1)|\varphi(N)$，$p-1$ 是偶数，所以 $\varphi(N)$ 是偶数.

(ii) 证：若 $a=1$ 或 $b=1$，则等式显然成立. 现设 $a>1$，$b>1$. 由于 $(a, b)=1$，所以 a 和 b 没有共同的素因子. 假设 a，b 的标准分解式为：

$$a = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_i^{\alpha_i},$$
$$b = p_{i+1}^{\alpha_{i+1}}p_{i+2}^{\alpha_{i+2}}\cdots p_k^{\alpha_k}.$$

这里 $\alpha_j \geqslant 1$，$1 \leqslant j \leqslant k$. 由引理 14 分别得到：

$$\varphi(a)=a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_i}\right),$$

$$\varphi(b)=b\left(1-\frac{1}{p_{i+1}}\right)\left(1-\frac{1}{p_{i+2}}\right)\cdots\left(1-\frac{1}{p_k}\right),$$

而

$$\varphi(ab)=ab\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right),$$

所以

$$\varphi(ab)=\varphi(a)\cdot\varphi(b).$$

5. 证：若 $N=2$，则 $\varphi(N)=\varphi(2)=1$，所以

$$\frac{1}{2}N\cdot\varphi(N)=\frac{1}{2}\cdot 2\cdot 1=1.$$

而不大于 2 且与 2 互素的数只有一个 1，因此 $N=2$ 的情形得到了证明.

现在假定 $N>2$. 不大于N且与N互素的正整数共有 $\varphi(N)$ 个，显然它们都小于 N. 由第 4 题知 $\varphi(N)$ 是偶数. 假如 n 是其中的一个数，即 $0<n<N$，$(n, N)=1$，那么必然有 $(N-n, N)=1$，且 $0<N-n<N$. 即 $N-n$ 也是这 $\varphi(N)$ 个数中的一个数，而且 $N-n\neq n$. 因此，可以把不大于N且与N互素的 $\varphi(N)$ 个数分成 $\frac{1}{2}\varphi(N)$ 个组，每组包含二个数，并且它们的和是 N. 所以，所有不大于N且与N互素的 $\varphi(N)$ 个数的和是 $\frac{1}{2}N\cdot\varphi(N)$.

6. 证：设 $1<a_2<\cdots<a_{\varphi(m)}$ 是不大于m而和m互素的全体正整数. 因 $b_1, b_2, \cdots, b_{\varphi(m)}$ 是模m的简化剩余系，$(a, m)=1$，由引理 13 可知 $ab_1, ab_2, \cdots, ab_{\varphi(m)}$ 也是模m的一个简化剩余系. 而 $ab_i\equiv r_i \pmod m$，$0\leqslant r_i<m$，所以 $r_1, r_2, \cdots, r_{\varphi(m)}$ 和 $1, a_2, \cdots, a_{\varphi(m)}$ 只在顺序上可能有不同.

因此

$$r_1+r_2+\cdots+r_{\varphi(m)}=1+a_2+\cdots+a_{\varphi(m)}.$$

由第5题知

$$1+a_2+\cdots+a_{\varphi(m)}=\frac{1}{2}m\cdot\varphi(m),$$

所以

$$\frac{1}{m}(r_1+r_2+\cdots+r_{\varphi(m)})$$

$$=\frac{1}{m}(1+a_2+\cdots+a_{\varphi(m)})=\frac{1}{2}\varphi(m).$$

7. 证：由于$x_1, x_2, \cdots, x_k$分别通过了$\varphi(m_1), \varphi(m_2), \cdots, \varphi(m_k)$个数，所以$M_1x_1+M_2x_2+\cdots+M_kx_k$通过$\varphi(m_1)\varphi(m_2)\cdots\varphi(m_k)$个数. 因$m_1, m_2, \cdots, m_k$两两互素，由第四题的(ii)推广到多个乘因子的情形，有

$$\varphi(m_1)\varphi(m_2)\cdots\varphi(m_k)=\varphi(m_1m_2\cdots m_k).$$

因而

$$M_1x_1+M_2x_2+\cdots+M_kx_k$$

恰好通过$\varphi(m_1m_2\cdots m_k)$个数. 现在来证明这些数与模$m_1m_2\cdots m_k$互素. 从$M_1, M_2, \cdots, M_k$的定义可知它们之中除了$M_i$外都是$m_i$的倍数，$1\leqslant i\leqslant k$. 因此

$$M_1x_1+M_2x_2+\cdots+M_kx_k=M_ix_i+m_iq,$$

这里q是整数. 由第一章引理8得

$$(M_1x_1+M_2x_2+\cdots+M_kx_k, m_i)=(M_ix_i, m_i).$$

由于x_i是模m_i的简化剩余系中的一个数，所以$(x_i, m_i)=1$. 而$M_i=m_1\cdots m_{i-1}m_{i+1}\cdots m_k$，且$m_1, \cdots, m_k$两两互素，所以$(M_i, m_i)=1$. 由此得

$$(M_ix_i, m_i)=1.$$

因此

$$(M_1x_1+M_2x_2+\cdots+M_kx_k, m_i)=1,$$

这里 i 可以取 $1, 2, \cdots, k$. 所以由互素的性质得

$$(M_1x_1 + M_2x_2 + \cdots + M_kx_k, m_1m_2\cdots m_k) = 1.$$

因此

$$M_1x_1 + M_2x_2 + \cdots + M_kx_k$$

通过了 $\varphi(m_1m_2\cdots m_k)$ 个与 $m_1m_2\cdots m_k$ 互素的数. 用与第 2 题相同的方法可以证明这 $\varphi(m_1m_2\cdots m_k)$ 个数是对模 $m_1m_2\cdots m_k$ 两两不同余的. 由引理 12 就证明了 $M_1x_1 + M_2x_2 + \cdots + M_kx_k$ 通过模 $m_1m_2\cdots m_k$ 的简化剩余系.

8. (i) 解: 由 $9450 = 2 \cdot 3^3 \cdot 5^2 \cdot 7$, 并由引理 14 得出

$$\varphi(N) = 9450\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right)$$

$$= \frac{2 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 2 \cdot 4 \cdot 6}{2 \cdot 3 \cdot 5 \cdot 7} = 2160.$$

(ii) 解: 设不大于 9450 且与 9450 互素的全体正整数的和是 S, 由第 5 题可得

$$S = \frac{1}{2} \cdot 9450 \cdot \varphi(9450)$$

$$= \frac{1}{2} \times 9450 \times 2160$$

$$= 10206000.$$

9. (i) 解: 由于 $\varphi(21) = (3-1)(7-1) = 12$, 而 $121^6 = 11^{12}$, 且 $(11, 21) = 1$. 由定理 1, $11^{12} \equiv 1 \pmod{21}$, 所以 $21 \mid (121^6 - 1)$.

(ii) 解: 因 $\varphi(13) = 12$, 而 $4965 = 413 \times 12 + 9$. 由定理 2, $8^{12} \equiv 1 \pmod{13}$, 所以 $8^{4965} \equiv 8^9 \pmod{13}$. 又 $8^2 \equiv -1 \pmod{13}$, 所以 $8^9 = 8^8 \cdot 8 \equiv 8 \pmod{13}$. 因而

$$8^{4965} \equiv 8 \pmod{13}.$$

(iii) 证: 由于 $p \neq 2, 5$, 所以 $(10, p) = 1$. 于是 $(10^k, p) = 1$. 由定理 2 得 $(10^k)^{p-1} \equiv 1 \pmod{p}$, 而

$$(10^k)^{p-1}-1=\underbrace{99\cdots9}_{(p-1)k\text{个}},$$

所以

$$p\mid\underbrace{99\cdots9}_{(p-1)k\text{个}}.$$

10. 证：$F_5=2^{2^5}+1=2^{32}+1$. 由 $640=5\cdot2^7$, 所以

$$5\cdot2^7\equiv-1\ (\mathrm{mod}\ 641).$$

根据引理 3 得到

$$5^4\cdot2^{28}\equiv1\ (\mathrm{mod}\ 641).$$

但

$$5^4=625\equiv-2^4\ (\mathrm{mod}\ 641),$$

因而

$$-2^4\cdot2^{28}\equiv1\ (\mathrm{mod}\ 641).$$

即

$$641\mid(2^{32}+1).$$

11. 证：若 $p\mid a$, $p\mid b$, 结论显然成立. 若 a 和 b 二者之一能整除 p, 不妨设 $p\mid b$, 则

$$(a+b)^p=a^p+bq_1\equiv a^p\ (\mathrm{mod}\ p),\quad q_1\text{ 是整数};$$

而 $a^p+b^p\equiv a^p(\mathrm{mod}\ p)$, 因而结论也成立. 现在假设 $p\nmid a$, $p\nmid b$. 由定理 2 得

$$a^{p-1}\equiv1\ (\mathrm{mod}\ p),\qquad b^{p-1}\equiv1\ (\mathrm{mod}\ p).$$

所以 $$a^p\equiv a\ (\mathrm{mod}\ p),\qquad b^p\equiv b\ (\mathrm{mod}\ p).$$

由第四章引理 4 可得

$$a^p+b^p\equiv a+b\ (\mathrm{mod}\ p).$$

因而只需证明

$$(a+b)^p\equiv a+b\ (\mathrm{mod}\ p).$$

若 $p\mid(a+b)$, 上同余式显然成立.

若 $p\nmid(a+b)$, 用定理 2 $(a+b)^{p-1}\equiv1\ (\mathrm{mod}\ p)$, 所以上同余式也成立. 因此，对任意整数 a 和 b 结论均成立.

不难把此题的结果推广为

$$(a_1+a_2+\cdots+a_n)^p\equiv a_1^p+a_2^p+\cdots+a_n^p \pmod p,$$

其中 $a_1, a_2, \cdots, a_n$ 是任意整数。

12. 解：$1978^n-1978^m=1978^m(1978^{n-m}-1)$

$$=2^m\cdot 989^m(1978^{n-m}-1).$$

又 1978^n 和 1978^m 的最后三位数相等，所以 1978^n-1978^m 的最后三位数都是 0。因此 1978^n-1978^m 被 1000 整除。而 $1000=2^3\cdot 5^3$。因而

$$2^3\cdot 5^3|2^m\cdot 989^m(1978^{n-m}-1).$$

由于 989^m 和 $1978^{n-m}-1$ 都是奇数，所以 $2^3|2^m$。m 的最小可能值为3。

又 $(5^3, 2^m\cdot 989^m)=1$，所以有 $5^3|(1978^{n-m}-1)$，即

$$1978^{n-m}\equiv 1 \pmod{125}.$$

问题变成找到使上式成立的最小正整数 $n-m$，这时取 $m=3$，$n+m=(n-m)+2m$ 也为最小。

由于 $\varphi(125)=5^2\cdot 4=100$，$(1978, 125)=1$，由定理 1 得到

$$1978^{100}\equiv 1 \pmod{125}.$$

我们可以证明 $(n-m)|100$。因为否则有：

$$100=(n-m)q+r,\quad q \text{ 是整数}, r \text{ 是正整数},$$

且 $0<r<n-m$，则

$$1978^{100}=1978^{(n-m)q}\cdot 1978^r\equiv 1978^r \pmod{125},$$

而

$$1978^{100}\equiv 1 \pmod{125}.$$

所以有

$$1978^r\equiv 1 \pmod{125}.$$

但 $r<n-m$，这与假定 $n-m$ 是使同余式成立的最小正整数相矛盾。因此 $(n-m)|100$。

又由于 $125|(1978^{n-m}-1)$，因此 1978^{n-m} 的末位数必须是1或6. 容易验证：只在 $4|(n-m)$ 时 1978^{n-m} 的末位数是6. 所以 $n-m$ 是4的倍数，是100的约数，它只能取4，20，100这三个数之一.

因

$$1978^4=(125\times15+103)^4\equiv103^4\ (\mathrm{mod}\ 125),$$

$$103^2=(3+4\cdot5^2)^2\equiv3^2+2\cdot3\cdot4\cdot5^2$$

$$\equiv609\equiv-16\ (\mathrm{mod}\ 125),$$

$$103^4\equiv(-16)^2\equiv6\ (\mathrm{mod}\ 125),$$

所以

$$1978^4\not\equiv1\ (\mathrm{mod}\ 125).$$

而

$$1978^{20}=(1978^4)^5\equiv6^5\not\equiv1\ (\mathrm{mod}\ 125),$$

因此 $n-m$ 的最小值为100. 现取 $m=3$，故 $n=103$，$n+m=106$.

13. 解：假设 $a=12n+a_1$，n 是非负整数，$1\leqslant a_1<12$，则

$$a^{b^c}=(12n+a_1)^{b^c}\equiv a_1^{b^c}\ (\mathrm{mod}\ 12).$$

当 $a_1=1, 5, 7, 11$ 时，$a_1^2\equiv1\ (\mathrm{mod}\ 12)$.

所以

$$a_1^{2k}\equiv(a_1^2)^k\equiv1\ (\mathrm{mod}\ 12),\quad k\geqslant1;$$

$$a_1^{2k-1}=a_1\cdot a_1^{2k-2}\equiv a_1\ (\mathrm{mod}\ 12),\quad k\geqslant1.$$

因此，若 b 是偶数，则 b^c 是偶数，$a_1^{b^c}\equiv1\ (\mathrm{mod}\ 12)$，指针指一点钟. 若 b 是奇数，则 b^c 是奇数，$a_1^{b^c}\equiv a_1\ (\mathrm{mod}\ 12)$，指针指 a_1 点钟.

当 $a_1=4$ 时，由于 $4^k\equiv4\ (\mathrm{mod}\ 12)$，$k\geqslant1$，所以指针指4点钟.

当 $a_1=8$ 时，则

$$8^{2k}=64^k\equiv4^k\equiv4\ (\mathrm{mod}\ 12),\quad k\geqslant1;$$

而

$$8^{2k-1}=8\cdot 8^{2k-2}\equiv 32\ (\bmod 12)\equiv 8\ (\bmod 12),\quad k\geqslant 1.$$

因此，若 b 是偶数，则 b^c 是偶数，$a_1^{b^c}\equiv 4\ (\bmod 12)$，指针指 4 点钟；若 b 是奇数，则 b^c 是奇数，$a_1^{b^c}\equiv 8\ (\bmod 12)$，指针指 8 点钟。

当 $a_1=2$ 时，则 $2^1=2\ (\bmod 12)$；

$$2^{2k}=4^k\equiv 4\ (\bmod 12),\quad k\geqslant 1;$$

$$2^{2k+1}=2\cdot 2^{2k}\equiv 8\ (\bmod 12),\quad k\geqslant 1.$$

因此，若 $b=1$，则 $b^c=1$，$a_1^{b^c}\equiv 2\ (\bmod 12)$，指针指 2 点钟；若 b 是偶数，则 b^c 是偶数，$a_1^{b^c}\equiv 4\ (\bmod 12)$，指针指 4 点钟；若 b 是大于 1 的奇数，则 $a_1^{b^c}\equiv 8\ (\bmod 12)$，指针指 8 点钟。

当 $a_1=6$ 时，由于 $6\equiv 6\ (\bmod 12)$，及 $6^k\equiv 12\ (\bmod 12)$，$k>1$。因此，若 $b=1$，则 $a_1^{b^c}\equiv 6\ (\bmod 12)$，指针指 6 点钟；若 $b>1$，则 $a_1^{b^c}\equiv 12\ (\bmod 12)$，指针指 12 点钟。

当 $a_1=10$ 时，由于 $10\equiv 10\ (\bmod 12)$ 及 $10^k\equiv 4\ (\bmod 12)$，$k>1$。因此，若 $b=1$，则 $a_1^{b^c}\equiv 10\ (\bmod 12)$，指针指10点钟；若 $b>1$，则 $a_1^{b^c}\equiv 4\ (\bmod 12)$，指针指 4 点钟。

当 $a_1=9$ 时，由于 $9^k\equiv 9\ (\bmod 12)$，$k\geqslant 1$。因此，指针指 9 点钟。

当 $a_1=3$ 时，则 $3^{2k}=9^k\equiv 9\ (\bmod 12)$，$k\geqslant 1$；而 $3^{2k-1}=3\cdot 3^{2k-2}\equiv 3\ (\bmod 12)$，$k\geqslant 1$。因此，若 b 是偶数，则 b^c 是偶数，$a_1^{b^c}\equiv 9\ (\bmod 12)$，指针指 9 点钟；若 b 是奇数，则 b^c 是奇数，$a_1^{b^c}\equiv 3\ (\bmod 12)$，指针指 3 点钟。

第六章

1. (i) 解：由于 $6250=2\times 5^5$，所以 $\dfrac{371}{6250}$ 是有限分数，经计算得到

$$\frac{371}{6250}=0.05936.$$

(ii) 解：$\frac{190}{37}=5+\frac{5}{37}$. 由于$(10, 37)=1$，所以$\frac{5}{37}$是纯循环小数. 又$\varphi(37)=36$，而$10^2\not\equiv 1 \pmod{37}$，$10^3\equiv 1 \pmod{37}$，所以循环节的长度是3，经计算得到

$$\frac{190}{37}=5.\dot{1}3\dot{5}.$$

(iii) 解：由于$28=2^2\times 7$. 所以$\frac{13}{28}$是混循环小数. 又$\varphi(7)=6$，而 $10^2\not\equiv 1 \pmod 7$，$10^3\not\equiv 1 \pmod 7$，$10^6\equiv 1 \pmod 7$，所以循环节的长度是6，经计算得到

$$\frac{13}{28}=0.46\dot{4}2857\dot{1}.$$

(iv) 解：由于$875=5^3\times 7$，所以$\frac{a}{875}$是混循环小数. 由(iii)的计算知道循环节的长度是6，经计算得到

$$\frac{4}{875}=0.004\dot{5}7142\dot{8},$$

$$\frac{29}{875}=0.033\dot{1}4285\dot{7},$$

$$\frac{139}{875}=0.158\dot{8}5714\dot{2},$$

$$\frac{361}{875}=0.412\dot{5}7142\dot{8}.$$

2.(i) 解：$0.868=\frac{868}{1000}=\frac{217}{250}$.

(ii) 解：$0.\dot{8}365\dot{4}=\frac{83654}{10^5-1}=\frac{83654}{99999}$.

(iii) 解: $0.37\dot{6}8935\dot{4} = 0.37 + \frac{0.\dot{6}8935\dot{4}}{100}$

$$= 0.37 + \frac{689354}{100 \times (10^6 - 1)}$$

$$= \frac{37}{100} + \frac{689354}{99999900}$$

$$= \frac{37689317}{99999900}.$$

3. 证: 如果能够证明$\sqrt[n]{a}$不能表示成为分数，则 c 一定是一个无限不循环小数. 现在我们用反证法来证明本题: 假设

$$\sqrt[n]{a} = \frac{q}{r}, \quad (q, r) = 1,$$

则 $r^n a = q^n$.因此 $r^n | q^n$，所以 $r | q$. 由此，对于 r 的任一素因子 p 均有 $p | q$，但 $p | r$，所以 $p | (q, r)$. 由假设 $(q, r) = 1$，因而有 $p = 1$. 由于 p 是 r 的任一素因子，所以得到 $r = 1$. 于是 $\sqrt[n]{a} = q$ 是正整数，这和 $0 < c < 1$ 矛盾.

4. 证: 我们可以假定此方程只有非零根，即可以假设 $a_n \neq 0$. 因为如果此方程含有 m 重零根，则可以在方程两边除以 x^m 而得到一个常数项不为零的整系数方程.

设方程有一个有理根 $\frac{q}{r}$，$(q, r) = 1$. 把它代入方程得到

$$\left(\frac{q}{r}\right)^n + a_1\left(\frac{q}{r}\right)^{n-1} + \cdots + a_n = 0,$$

即

$$q^n + a_1 q^{n-1} r + \cdots + a_n r^n = 0.$$

所以

$$q^n = -r(a_1 q^{n-1} + a_2 q^{n-2} r + \cdots + a_n r^{n-1}).$$

由于上式右端括弧内是整数，所以 $r|q^n$. 对于 r 的任一素因子 p，有 $p|q^n$，故 $p|q$，但 $p|r$，所以 $p|(q, r)$. 由假定 $(q, r)=1$ 而得到 $p=1$. 由于 p 是 r 的任一素因子，所以有 $r=1$. 因而方程的任一有理根都是整数.

5. 证：若 $\log_{10}2=\dfrac{q}{r}$，$(q, r)=1$，则由对数的定义得 $10^{q/r}=2$，即 $10^q=2^r$. 所以 $5^q=2^{r-q}$. 由于 q 和 $r-q$ 是正整数，$(5, 2)=1$，因此上式不可能成立. 所以 $\log_{10}2$ 是无理数.

6. 证：假设 $\log_M N=\dfrac{q}{r}$，$(q, r)=1$. 由对数的定义可知：$M^{q/r}=N$，即 $M^q=N^r$. 设 M 和 N 的标准分解式分别是：

$$M=u_1^{\alpha_1}u_2^{\alpha_2}\cdots u_m^{\alpha_m}, N=v_1^{\beta_1}v_2^{\beta_2}\cdots v_n^{\beta_n}.$$

这里 $u_1<u_2<\cdots<u_m$，$u_1, u_2, \cdots, u_m$ 是不同的素数；$v_1<v_2<\cdots<v_n$，$v_1, v_2, \cdots, v_n$ 是不同的素数. 因而由 $M^q=N^r$ 得到

$$u_1^{\alpha_1 q}u_2^{\alpha_2 q}\cdots u_m^{\alpha_m q}=v_1^{\beta_1 r}v_2^{\beta_2 r}\cdots v_n^{\beta_n r}.$$

由算术基本定理，一个数的标准分解式是唯一的. 因此有 $m=n$，且 $u_i=v_i$，$\alpha_i q=\beta_i r(i=1, 2, \cdots, n)$.
于是

$$\frac{\alpha_i}{r}=\frac{\beta_i}{q}\quad(i=1, 2, \cdots, n).$$

所以令

$$S=u_1^{\alpha_1/r}u_2^{\alpha_2/r}\cdots u_m^{\alpha_m/r}=v_1^{\beta_1/q}v_2^{\beta_2/q}\cdots v_n^{\beta_n/q},$$

则 $M=S^r$，$N=S^q$. 这与假设 M 和 N 不能表示成同底数的乘幂相矛盾. 因此 $\log_M N\neq\dfrac{q}{r}$，于是证明了 $\log_M N$ 是无理数.

由此可知，$\log_2 5$，$\log_{16} 72$ 等等都是无理数。

7. 证：假设 $e=\frac{q}{r}$，$(q, r)=1$. 又设正整数 $k \geqslant r$，则有 $r \mid k!$. 并且对于任意不大于 k 的正整数 n，有 $n! \mid k!$. 所以当 $e=\frac{q}{r}$ 时

$$A=k!\left(e-1-\frac{1}{1!}-\frac{1}{2!}-\cdots-\frac{1}{k!}\right)$$

是整数，而由 e 的定义得

$$\begin{aligned}
0<A&=k!\left(\sum_{m=0}^{\infty}\frac{1}{m!}-1-\frac{1}{1!}-\frac{1}{2!}-\cdots-\frac{1}{k!}\right)\\
&=k!\left(\frac{1}{(k+1)!}+\frac{1}{(k+2)!}+\cdots\right)\\
&=\left(\frac{1}{k+1}+\frac{1}{(k+1)(k+2)}\right.\\
&\qquad\left.+\frac{1}{(k+1)(k+2)(k+3)}+\cdots\right)\\
&<\frac{1}{k+1}+\frac{1}{(k+1)^2}+\frac{1}{(k+1)^3}+\cdots\\
&=\frac{1}{k+1}\left(1+\frac{1}{k+1}+\frac{1}{(k+1)^2}+\cdots\right)\\
&=\frac{1}{k+1}\cdot\frac{1}{1-\frac{1}{k+1}}=\frac{1}{k}.
\end{aligned}$$

由于 $k \geqslant r \geqslant 1$，所以 A 不是整数. 这与前面得到的 A 是整数的结论相矛盾. 因此 e 是无理数.

8. 证：假设 $J=\frac{q}{r}$，$(q, r)=1$. 又设正整数 $k \geqslant r$，则有 $r \mid k!$. 所以当 $J=\frac{q}{r}$ 时

$$A = (2^k \cdot k!)^2\left[J - \left(1 - \frac{1}{2^2} + \frac{1}{2^2 \cdot 4^2} - \cdots + \frac{(-1)^k}{(2^k \cdot k!)^2}\right)\right]$$

是整数．而由 J 的定义得

$$0 < |A| = \left|(2^k \cdot k!)^2\left[\sum_{m=0}^{\infty}\frac{(-1)^m}{(2^m \cdot m!)^2} - \left(1 - \frac{1}{2^2} + \frac{1}{2^2 \cdot 4^2} - \cdots + \frac{(-1)^k}{(2^k \cdot k!)^2}\right)\right]\right|$$

$$\leqslant (2^k \cdot k!)^2\left(\frac{1}{[2^{k+1}(k+1)!]^2} + \frac{1}{[2^{k+2}(k+2)!]^2} + \cdots\right)$$

$$= \frac{1}{[2(k+1)]^2} + \frac{1}{[2^2(k+1)(k+2)]^2} + \cdots$$

$$< \frac{1}{2^2} + \frac{1}{2^4} + \frac{1}{2^6} + \cdots$$

$$= \frac{1}{2^2}\frac{1}{1 - \frac{1}{2^2}} = \frac{1}{3}.$$

所以 A 不是整数．因而 J 是无理数．

9. 证：当 $a < b$ 时，不存在不大于 a 而为 b 的倍数的正整数．而按定义 $\left[\frac{a}{b}\right] = 0$，所以结论成立．现假定 $a \geqslant b$．把所有不大于 a 而为 b 的倍数的正整数排列成

$$b, 2b, 3b, \cdots, Sb.$$

Sb 是其中最大者，则 $Sb \leqslant a < (S+1)b$．因此

$$S \leqslant \frac{a}{b} < S + 1,$$

所以

$$S = \left[\frac{a}{b}\right].$$

10. 证：当 $p^k > n$ 时，$\left[\frac{n}{p^k}\right] = 0$，所以 S 只含有有限个不等于 0 的项。

若 $n < p$，则 $n!$ 的标准分解式中不含有 p，而按定义 $S = 0$，所以结论成立。

现假设 $n \geqslant p$，由上一题可知，在 $1, 2, 3, \cdots, n$ 这 n 个数中，有 $\left[\frac{n}{p}\right]$ 个 p 的倍数，有 $\left[\frac{n}{p^2}\right]$ 个 p^2 的倍数…等等。所以恰好有 $\left[\frac{n}{p^r}\right] - \left[\frac{n}{p^{r+1}}\right]$ 个数是 p^r 的倍数而不是 p^{r+1} 的倍数。这样的数的分解式中 p 的方次数是 r。因此

$$S = \left(\left[\frac{n}{p}\right] - \left[\frac{n}{p^2}\right]\right) + 2\left(\left[\frac{n}{p^2}\right] - \left[\frac{n}{p^3}\right]\right) + 3\left(\left[\frac{n}{p^3}\right] - \left[\frac{n}{p^4}\right]\right) + \cdots$$

$$= \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots.$$

11. 解：由上题的结果有

$$k = \left[\frac{1000}{3}\right] + \left[\frac{1000}{9}\right] + \left[\frac{1000}{27}\right] + \left[\frac{1000}{81}\right] + \left[\frac{1000}{243}\right] + \left[\frac{1000}{729}\right]$$

$$= 333 + 111 + 37 + 12 + 4 + 1 = 498.$$

12. (i) 证：由 C_m^n 的定义有

$$C_m^{m-n} = \frac{m!}{(m-n)!\,[m-(m-n)]!} = \frac{m!}{n!\,(m-n)!} = C_m^n.$$

(ii) 证：$C_m^n = \frac{m!}{n!\,(m-n)!}$，由于 $n \leqslant m$，$m - n \leqslant m$，

所以如有素数 $p|n!(m-n)!$，必有 $p|m!$． 也就是分母的素因子 p 必定能除尽分子．下面只需证明，在分子和分母的标准分解式中，分母中的 p 的方次数不大于分子中的 p 的方次数．

由于 $[\alpha+\beta]\geqslant[\alpha]+[\beta]$，以及 $m=n+(m-n)$，所以

$$\left[\frac{m}{p^r}\right]\geqslant\left[\frac{n}{p^r}\right]+\left[\frac{m-n}{p^r}\right],$$

$$\sum_{r=1}^{\infty}\left[\frac{m}{p^r}\right]\geqslant\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]+\sum_{r=1}^{\infty}\left[\frac{m-n}{p^r}\right].$$

由第 10 题知上式左端为 $m!$ 中含有的 p 的方次数，右端两项分别为 $n!$ 和 $(m-n)!$ 中含有的 p 的方次数，所以 C_m^n 是正整数．

(iii) 证：设 $(n+1)(n+2)\cdots(n+k)$ 是 k 个连续正整数的乘积．由于

$$\frac{(n+1)(n+2)\cdots(n+k)}{k!}=\frac{(n+k)!}{k!\,n!}=C_{n+k}^k,$$

由(ii) 知 C_{n+k}^k 是整数，所以 $k!\,|(n+1)(n+2)\cdots(n+k)$．

(iv) 证：由(iii)，当 $1\leqslant k\leqslant p-1$ 时

$$k!\,|p(p-1)\cdots(p-k+1),$$

但是因 $(k!,p)=1$，所以

$$k!\,|(p-1)(p-2)\cdots(p-k+1).$$

而

$$C_p^k=\frac{p!}{k!(p-k)!}=p\cdot\frac{(p-1)(p-2)\cdots(p-k+1)}{k!}.$$

由此得到 $p|C_p^k$．

13. (i) 证：当 $p=2$ 时结论显然成立． 现假设 p 是奇素数． 若取 x_0 是 $1,2,\cdots,p-1$ 中的一个数时，则由于 $(x_0,p)=1$ 及第四章引理 12，同余式 $x_0x\equiv1\pmod p$ 有解，

它的最小非负整数解也在 1, 2, $\cdots$, $p-1$ 中. 当 $x=x_0$ 时由 $x^2\equiv 1\pmod p$ 得 $(x-1)(x+1)\equiv 0\pmod p$. 这时最小正数解是 $x=1$ 和 $x=p-1$. 因此, 当 x_0 是数列 2, 3, $\cdots$, $p-2$ 中的任一数时, 同余式 $x_0x\equiv 1\pmod p$ 的最小正数解 x 必是同一数列中不等于 x_0 的另一个数. 所以可以把数列 2, 3, $\cdots$, $p-2$ 分成 $\frac{p-3}{2}$ 个组, 每个组包含二个数, 当 x_0, x 分别取作这二个数时, 同余式 $x_0x\equiv 1\pmod p$ 成立. 由第四章引理 6, 把这 $\frac{p-3}{2}$ 个同余式相乘就得到

$$2\cdot 3\cdots(p-2)\equiv 1\pmod p.$$

又

$$(p-1)\equiv -1\pmod p,$$

所以

$$(p-1)!\equiv -1\pmod p.$$

(ii) 证: 假如 p 不是素数, 则必有约数 $d|p$, $1<d<p$, 因此 $(p-1)!\equiv -1\pmod d$. 但 $d|(p-1)!$, 所以又有 $(p-1)!\equiv 0\pmod d$. 两同余式矛盾. 因而 p 必定是素数.

14. 证: 假若

$$4[(n-1)!+1]+n\equiv 0\ [\mathrm{mod}\ n(n+2)],\quad n>1 \quad (1)$$

成立. 可以证明 n 必为奇数, 即 $(4, n)=1$. 因为容易验证 $n=2, 4$ 不满足 (1) 式. 而当 $n=2m$, $m>2$ 时, 由 (1) 式得 $n|4[(n-1)!+1]$, 于是 $m|2[(2m-1)!+1]$. 而 $m>2$ 时 $2m-1>m$, 所以 $m|(2m-1)!$, 故 $m\nmid[(2m-1)!+1]$, 于是 $m|2$. 但这和假设 $m>2$ 矛盾, 因此证明了 $(4, n)=1$. 于是由 (1) 式得到 $n|[(n-1)!+1]$, 也就是 $(n-1)!\equiv -1\pmod n$. 由第 13 题可知 n 是素数.

又由 (1) 式可知

$$(n+2)|\{4[(n-1)!+1]+n\},$$

于是

$$(n+2)\mid\{4[(n-1)!+1]-2\}.$$

由于 $n+2$ 也是奇数，所以

$$(n+2)\mid\{2[(n-1)!+1]-1\},$$

即

$$2(n-1)!\equiv -1\ [\bmod (n+2)]. \qquad (2)$$

又因 $n\equiv -2\ [\bmod (n+2)]$，所以

$$n(n+1)=n^2+n\equiv 2\ [\bmod (n+2)]. \qquad (3)$$

由 (2)，(3) 及第四章引理 6 得到

$$2(n+1)!\equiv -2\ [\bmod (n+2)].$$

由于 $n+2$ 是奇数，所以

$$(n+1)!\equiv -1\ [\bmod (n+2)].$$

因此由第 13 题可知 $n+2$ 是素数，于是证明了 n 和 $n+2$ 是孪生素数。

反之，假若 n 和 $n+2$ 都是素数，显然 $n\neq 2$，所以 n 是奇数。由 Wilson 定理

$$(n-1)!+1\equiv 0\ (\bmod n),$$

所以

$$4[(n-1)!+1]+n\equiv 0\ (\bmod n). \qquad (4)$$

又由 (3) 式得到

$$(n+1)!\equiv 2(n-1)!\ [\bmod (n+2)],$$

因此

$$\begin{aligned}4[(n-1)!+1]+n&=4(n-1)!+(n+2)+2\\&\equiv 2(n+1)!+2\ [\bmod (n+2)]. \qquad (5)\end{aligned}$$

又因 $n+2$ 是素数，由 Wilson 定理可得

$$(n+1)!+1\equiv 0\ [\bmod (n+2)]. \qquad (6)$$

由 (5)，(6) 及第四章引理 3 得

$$4[(n-1)!+1]+n\equiv 0\ [\bmod (n+2)]. \qquad (7)$$

由 (4)，(7) 两式及 $(n, n+2)=1$ 而得到

$$4[(n-1)!+1]+n\equiv 0\ [\bmod n(n+2)].$$

15. 证：由 $a^{m-1}\equiv 1\ (\bmod m)$ 可知 $(a, m)=1$. 由第五章定理 1 有

$$a^{\varphi(m)}\equiv 1\ (\bmod m).$$

设 d 是同余式 $a^x\equiv 1\ (\bmod m)$ 的最小正整数解，则必定有 $d\mid\varphi(m)$，因为否则可写成 $\varphi(m)=dq+r$，$0<r<d$. 这时由

$$a^{\varphi(m)}=a^{dq+r}\equiv 1\ (\bmod m)$$

及假定 $a^d\equiv 1\ (\bmod m)$，可以得到 $a^r\equiv 1\ (\bmod m)$. 这与假设 d 是 $a^x\equiv 1\ (\bmod m)$ 的最小正数解矛盾. 所以 $d\mid\varphi(m)$. 用同样的方法由 $a^{m-1}\equiv 1\ (\bmod m)$ 可以证明 $d\mid m-1$. 由于除 $m-1$ 外所有 $m-1$ 的约数都不是 $a^x\equiv 1\ (\bmod m)$ 的解，因此有 $d=m-1$. 所以 $(m-1)\mid\varphi(m)$. 设若 m 不是素数，$p_1, p_2, \cdots, p_n$ 是 m 的素因数，$n>1$，则 $p_i<m$，$1\leqslant i\leqslant n$. 因此

$$\begin{aligned}\varphi(m)&=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_n}\right)\\&<m\left(1-\frac{1}{m}\right)^n<m\left(1-\frac{1}{m}\right)=m-1.\end{aligned}$$

这与 $(m-1)\mid p(m)$ 矛盾. 所以 m 一定是素数.

16. (i) 证：设 d 是 n 的约数，$d=q_1^{r_1}q_2^{r_2}\cdots q_m^{r_m}$ 是它的标准分解式，则有

$$q_1^{r_1}q_2^{r_2}\cdots q_m^{r_m}\mid p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}.$$

由于标准分解式是唯一的，所以每一个 q_i 必定是 $p_1, p_2, \cdots, p_n$ 之一，且 $m\leqslant n$. 若 $q_i=p_j$，必有 $r_i\leqslant\alpha_j$. 因此 n 的约数 d 必定有如下的形式

$$d=p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n},$$

这里 $0\leqslant\beta_1\leqslant\alpha_1$, $0\leqslant\beta_2\leqslant\alpha_2, \cdots, 0\leqslant\beta_n\leqslant\alpha_n$. 每一个约数 d 对应着一组 $\beta_1, \beta_2, \cdots, \beta_n$. 而且不全相同的组 $\beta_1, \beta_2, \cdots, \beta_n$，对应着不同的约数. 现 β_1 可取 $0, 1, \cdots, \alpha_1$ 共 α_1+1

个值，β_2 可取 α_2+1 个值，$\cdots$，β_n 可取 α_n+1 个值．所以总共有 $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_n+1)$ 组不完全相同的 $\beta_1,\beta_2,\cdots,\beta_n$．因此约数的个数有 $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_n+1)$ 个．

(ii) 证：容易看出乘积

$$(p_1^0+p_1^1+p_1^2+\cdots+p_1^{\alpha_1})(p_2^0+p_2^1+p_2^2+\cdots+p_2^{\alpha_2})\cdots$$
$$\cdots(p_n^0+p_n^1+p_n^2+\cdots+p_n^{\alpha_n})$$

展开后是 $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_n+1)$ 项的和，每一项是每一括弧中取出一项的乘积，因此具有形式：$p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$，并且 $0\leqslant\beta_1\leqslant\alpha_1$，$0\leqslant\beta_2\leqslant\alpha_2,\cdots$，$0\leqslant\beta_n\leqslant\alpha_n$．所以每一项都是 n 的约数．由 (i) 可知展开后的 $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_n+1)$ 项恰好是 n 的全部约数．因此

$$\sigma(n)=(p_1^0+p_1^1+\cdots+p_1^{\alpha_1})(p_2^0+p_2^1+\cdots+p_2^{\alpha_2})$$
$$\cdots(p_n^0+p_n^1+\cdots+p_n^{\alpha_n}).$$

由于

$$(p_i-1)(p_i^0+p_i^1+\cdots+p_i^{\alpha_i})=p_i^{\alpha_i+1}-1,\quad 1\leqslant i\leqslant n,$$

所以

$$\sigma(n)=\left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{\alpha_2+1}-1}{p_2-1}\right)\cdots\left(\frac{p_n^{\alpha_n+1}-1}{p_n-1}\right).$$

17. 证：若 n 是素数，则 $\varphi(n)=n-1$，且 $\sigma(n)=n+1$．所以满足 $\varphi(n)\mid(n-1)$，$(n+1)\mid\sigma(n)$．

反之，如果 $\varphi(n)\mid(n-1)$，且 $(n+1)\mid\sigma(n)$，若 $n=2^m$，则 $\varphi(n)=2^m-2^{m-1}=2^{m-1}$ 而 $n-1=2^m-1$．当 $m>1$ 时 2^{m-1} 是偶数，2^m-1 是奇数，因而 $\varphi(n)\mid(n-1)$ 不成立．所以只能 $m=1$．这时 $n=2$ 是素数．若 n 含有奇素因子 p_i，由第五章引理 14 知 $(p_i^{\alpha_i}-p_i^{\alpha_i-1})\mid\varphi(n)$，这里 α_i 是 n 的标准分解式中 p_i 的方次数．由于 $p_i^{\alpha_i}-p_i^{\alpha_i-1}$ 是偶数，所以 $\varphi(n)$ 是偶数．因而由 $\varphi(n)\mid(n-1)$ 可知 n 是奇数．假设 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_m^{\alpha_m}$，$p_1,p_2,\cdots,p_m$ 为不同的奇素数，由

$(\varphi n) | (n-1)$ 及 $(p_i^{\alpha_i} - p_i^{\alpha_i-1}) | \varphi(n)$，$1 \leqslant i \leqslant m$，得到

$$(p_i^{\alpha_i} - p_i^{\alpha_i-1}) | (p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} - 1).$$

所以

$$p_i^{\alpha_i-1} | (p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} - 1).$$

由于 $p_i^{\alpha_i-1} | p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$，因此 $p_i^{\alpha_i-1} | 1$. 于是 $\alpha_i = 1$，$1 \leqslant i \leqslant m$. 所以 $n = p_1 p_2 \cdots p_m$.

这时

$$\varphi(n) = (p_1 - 1)(p_2 - 1) \cdots (p_m - 1),$$
$$\sigma(n) = (p_1 + 1)(p_2 + 1) \cdots (p_m + 1).$$

由于 $p_1, p_2, \cdots, p_m$ 都是奇素数，故 $2 | (p_i - 1)$，$2 | (p_i + 1)$，$i = 1, 2, \cdots, m$. 所以得到

$$2^m | \varphi(n), \quad 2^m | \sigma(n).$$

由 $\varphi(n) | (n-1)$ 和 $(n+1) | \sigma(n)$ 可知 $n = 2^m k + 1$ 且 $2^{m-1}(n+1) | \sigma(n)$，但是用数学归纳法不难证明当 $m \geqslant 2$ 时，$2^{m-1}(n+1) > \sigma(n)$（$n = p_1 p_2 \cdots p_m$ 时）. 因此 $m = 1$，n 是素数.

第七章

1.（i）证：当 $n = 1$ 时，由于 $1 \cdot 2 = \frac{1}{3} \cdot 1 \cdot 2 \cdot 3$，故命题成立. 设 k 是 $\geqslant 2$ 的整数，假设命题对于 $n = k - 1$ 成立，即假定

$$1 \cdot 2 + 2 \cdot 3 + \cdots + (k-1)k = \frac{1}{3}(k-1) \cdot k \cdot (k+1),$$

则当 $n = k$ 时，由归纳法的假定有

$$\begin{aligned} & 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + (k-1) \cdot k + k(k+1) \\ &= \frac{1}{3}(k-1) \cdot k \cdot (k+1) + k(k+1) \\ &= k(k+1)\left[\frac{1}{3}(k-1) + 1\right] \\ &= \frac{1}{3} k(k+1)(k+2). \end{aligned}$$

所以 n 为任意正整数时命题成立.

(ii) 证: 当 $n=1$ 时 $1^3=\left(\frac{1\cdot 2}{2}\right)^2$, 故命题成立. 设 k 是 $\geqslant 2$ 的整数,假设命题对于 $n=k-1$ 成立,即假定

$$1^3+2^3+\cdots+(k-1)^3=\left[\frac{(k-1)k}{2}\right]^2,$$

则当 $n=k$ 时,由归纳法的假定

$$\begin{aligned}&1^3+2^3+\cdots+(k-1)^3+k^3\\&=\left[\frac{(k-1)k}{2}\right]^2+k^3=k^2\left[\left(\frac{k-1}{2}\right)^2+k\right]\\&=k^2\frac{k^2-2k+1+4k}{4}=\left[\frac{k(k+1)}{2}\right]^2.\end{aligned}$$

所以 n 为任意正整数时命题成立.

(iii) 证: 设 $f(n)=a^{n+2}+(a+1)^{2n+1}$. 当 $n=0$ 时 $f(0)=a^2+a+1$, 故命题成立. 假设命题对于 $n=k-1$ 成立,即假定 $(a^2+a+1)|f(k-1)$, 则当 $n=k$ 时,

$$\begin{aligned}f(k)&=a^{k+2}+(a+1)^{2k+1}\\&=a\cdot a^{k+1}+(a+1)^2\cdot(a+1)^{2k-1}\\&=a\cdot a^{k+1}+(a^2+a+1)(a+1)^{2k-1}+a(a+1)^{2k-1}\\&=a[a^{k+1}+(a+1)^{2k-1}]+(a^2+a+1)(a+1)^{2k-1}\\&=af(k-1)+(a^2+a+1)(a+1)^{2k-1}.\end{aligned}$$

由归纳法的假定, $(a^2+a+1)|f(k-1)$. 所以由上式可知 $(a^2+a+1)|f(k)$. 命题得证.

(iv) 求证

$$(a_1a_2\cdots a_n)^{1/n}\leqslant\frac{a_1+a_2+\cdots+a_n}{n}, \quad (1)$$

这里 $a_1, a_2, \cdots, a_n$ 是非负实数.

证: 当 $n=1$ 时,由 $a_1=a_1$, 命题成立. 又若 $a_1, a_2, \cdots, a_n$ 中有一个等于 0, 命题显然也成立,因此可以假设

$$0 < a_1 \leqslant a_2 \leqslant \cdots \leqslant a_n. \tag{2}$$

若 $a_1 = a_n$，则所有的 $a_j(j = 1, 2, \cdots, n)$ 都相等，容易验证命题也成立．所以可以进一步假设 $a_1 < a_n$．假设 $n = k - 1$ 时命题成立，即假定

$$(a_1 a_2 \cdots a_{k-1})^{1/k-1} \leqslant \frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1}, \tag{3}$$

则当 $n = k$ 时

$$\frac{a_1 + a_2 + \cdots + a_k}{k}$$

$$= \frac{(k-1)\dfrac{a_1 + a_2 + \cdots + a_{k-1}}{k-1} + a_k}{k}$$

$$= \frac{k \cdot \dfrac{a_1 + a_2 + \cdots + a_{k-1}}{k-1} + a_k - \dfrac{a_1 + a_2 + \cdots + a_{k-1}}{k-1}}{k}$$

$$= \frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1} + \frac{a_k - \dfrac{a_1 + a_2 + \cdots + a_{k-1}}{k-1}}{k}. \tag{4}$$

由假设 $a_1 < a_n$，$n = k$ 及 (2) 式可知

$$\frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1} < \frac{(k-1)a_k}{k-1} = a_k.$$

所以 (4) 式右端两项均大于零，将 (4) 式两边乘方 k $(k \geqslant 2)$ 次，并且利用不等式

$$(a + b)^k > a^k + k a^{k-1} b \ (k \geqslant 2,\ a > 0,\ b > 0)$$

（这个不等式用数学归纳法很容易加以证明），得到

$$\left(\frac{a_1 + a_2 + \cdots + a_k}{k}\right)^k > \left(\frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1}\right)^k$$

$$+ k\left(\frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1}\right)^{k-1}$$

$$\times\left(\frac{a_k-\dfrac{a_1+a_2+\cdots+a_{k-1}}{k-1}}{k}\right)$$

$$=\left(\frac{a_1+a_2+\cdots+a_{k-1}}{k-1}\right)^{k-1}\cdot a_k.$$

由归纳法的假定(3)式可知上式右端 $\geqslant a_1a_2\cdots a_k$，所以

$$(a_1a_2\cdots a_k)^{1/k}\leqslant\frac{a_1+a_2+\cdots+a_k}{k}.$$

命题得证.

2.（i）解:

$$\frac{50}{13}=3+\frac{11}{13}=3+\frac{1}{\dfrac{13}{11}}=3+\frac{1}{1+\dfrac{2}{11}}$$

$$=3+\frac{1}{1+\dfrac{1}{\dfrac{11}{2}}}=3+\frac{1}{1+\dfrac{1}{5+\dfrac{1}{2}}}$$

$$=[3,1,5,2].$$

(ii) 解:

$$-\frac{53}{25}=-3+\frac{22}{25}=-3+\frac{1}{\dfrac{25}{22}}$$

$$=-3+\frac{1}{1+\dfrac{3}{22}}=-3+\frac{1}{1+\dfrac{1}{\dfrac{22}{3}}}$$

$$=-3+\frac{1}{1+\dfrac{1}{7+\dfrac{1}{3}}}=[-3,1,7,3].$$

3. 解：因为 $6<\sqrt{41}<7$，所以

$$\sqrt{41}=6+(\sqrt{41}-6)=6+\cfrac{1}{\cfrac{1}{\sqrt{41}-6}}$$

$$=6+\cfrac{1}{\cfrac{\sqrt{41}+6}{5}}.$$

又 $2<\frac{\sqrt{41}+6}{5}<3$，所以有

$$\frac{\sqrt{41}+6}{5}=2+\frac{\sqrt{41}-4}{5}=2+\cfrac{1}{\cfrac{5}{\sqrt{41}-4}}$$

$$=2+\cfrac{1}{\cfrac{\sqrt{41}+4}{5}}.$$

又 $2<\frac{\sqrt{41}+4}{5}<3$，所以

$$\frac{\sqrt{41}+4}{5}=2+\frac{\sqrt{41}-6}{5}=2+\cfrac{1}{\cfrac{5}{\sqrt{41}-6}}$$

$$=2+\frac{1}{\sqrt{41}+6}.$$

又 $12<\sqrt{41}+6<13$，所以

$$\sqrt{41}+6=12+(\sqrt{41}-6)$$

$$=12+\cfrac{1}{\cfrac{1}{\sqrt{41}-6}}=12+\cfrac{1}{\cfrac{\sqrt{41}+6}{5}}.$$

最后的分式与前面第一个式子中的最后分式相同，所以就得

到 $\sqrt{41}$ 的循环连分数表示式

$$\sqrt{41}=6+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{12+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{12+\cdots}}}}}}$$

$$=[6,\dot{2},2,1\dot{2}].$$

它的最初几个渐近分数是

$$\frac{p_1}{q_1}=6,\quad \frac{p_2}{q_2}=\frac{13}{2}=6.5,$$

$$\frac{p_3}{q_3}=\frac{32}{5}=6.4,\quad \frac{p_4}{q_4}=\frac{397}{62}=6.403225\cdots,$$

$$\frac{p_5}{q_5}=\frac{826}{129}=6.403100\cdots,$$

$$\frac{p_6}{q_6}=\frac{2049}{320}=6.403125\cdots.$$

由引理5可知

$$6.403100<\sqrt{41}<6.403125.$$

4. 解：由引理1得到

$$\frac{p_1}{q_1}=\frac{3}{1},\quad \frac{p_2}{q_2}=\frac{3\times 7+1}{7}$$

$$=\frac{22}{7}=3.14285714\cdots,$$

$$\frac{p_3}{q_3}=\frac{22\times 15+3}{7\times 15+1}=\frac{333}{106}=3.141509433\cdots,$$

$$\frac{p_4}{q_4}=\frac{333\times 1+22}{106\times 1+7}=\frac{355}{113}=3.141592920\cdots,$$

$$\frac{p_5}{q_5}=\frac{355\times 292+333}{113\times 292+106}$$

$$=\frac{103993}{33102}=3.141592653011\cdots,$$

$$\frac{p_6}{q_6}=\frac{103993\times 1+355}{33102\times 1+113}$$

$$=\frac{104348}{33215}=3.141592653921\cdots,$$

$$\frac{p_7}{q_7}=\frac{104348\times 1+103993}{33215\times 1+33102}$$

$$=\frac{208341}{66317}=3.14159265346\cdots.$$

所以

$$3.1415926534<\pi<3.1415926540.$$

5. 证：因 $\frac{a}{|b|}=\frac{p_k}{q_k}$，由引理 2 得

$$aq_{k-1}-|b|p_{k-1}=(-1)^k.$$

等式两边各乘以 $(-1)^k c$，得

$$a[(-1)^k cq_{k-1}]+|b|[(-1)^{k+1}cp_{k-1}]=c,$$

即

$$a[(-1)^k cq_{k-1}]+b\cdot\frac{|b|}{b}[(-1)^{k+1}cp_{k-1}]=c.$$

所以 (x_0, y_0) 是一组整数解。

6. (i) 解：把 $\frac{43}{15}$ 化成连分数，得

$$\frac{43}{15}=2+\cfrac{1}{1+\cfrac{1}{6+\cfrac{1}{2}}},$$

因此

$$k=4,\quad \frac{p_1}{q_1}=2,\quad \frac{p_2}{q_2}=3,\quad \frac{p_3}{q_3}=\frac{6\times 3+2}{6\times 1+1}=\frac{20}{7},$$

所以

$$\begin{cases}x_0=(-1)^4\times 8\times 7=56,\\ y_0=(-1)^5\times 8\times 20=-160\end{cases}$$

是一组特殊解．由第三章定理一，它的一般解是

$$\begin{cases}x=56-15t,\\ y=-160+43t.\end{cases}\quad (t=0,\pm 1,\pm 2,\cdots)$$

(ii) 解：把$\frac{10}{37}$化成连分数得

$$\frac{10}{37}=\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{3}}}},$$

因此

$$k=5,\qquad \frac{p_1}{q_1}=\frac{0}{1},\quad \frac{p_2}{q_2}=\frac{1}{3},$$

$$\frac{p_3}{q_3}=\frac{1\times 1+0}{1\times 3+1}=\frac{1}{4},$$

$$\frac{p_4}{q_4}=\frac{2\times 1+1}{2\times 4+3}=\frac{3}{11},$$

$$\frac{p_5}{q_5}=\frac{3\times 3+1}{3\times 11+4}=\frac{10}{37}.$$

所以

$$\begin{cases}x_0=(-1)^5\times 3\times 11=-33,\\ y_0=(-1)^5\times 3\times 3=-9\end{cases}$$

是一组整数解．它的一般解是

$$\begin{cases}x=-33+37t,\\ y=-9+10t.\end{cases}\quad (t=0,\pm 1,\pm 2,\cdots)$$

7.(i) 证：设 $n=2m+c$，$0\leqslant c\leqslant 1$，则

$$\sum_{k=1}^{n}\left[\frac{k}{2}\right]=\sum_{k=1}^{2m+c}\frac{k}{2}-\sum_{k=1}^{2m+c}\left\{\frac{k}{2}\right\}$$

$$=\frac{1}{4}(2m+c)(2m+c+1)-\frac{1}{2}(m+c)$$

$$=\frac{1}{4}\{(2m+c)^2+(2m+c)-2(m+c)\}$$

$$=\frac{1}{4}\{4m^2+4mc+c^2-c\}$$

$$=m^2+mc.$$

最后一步是由于 $c^2=c$. 又

$$\left[\frac{n^2}{4}\right]=\left[\frac{(2m+c)^2}{4}\right]=\left[m^2+mc+\frac{c^2}{4}\right]$$

$$=m^2+mc.$$

(ii) 证：设 $n=3m+c$，$0\leqslant c\leqslant 2$，则

$$\sum_{k=1}^{n}\left[\frac{k}{3}\right]=\sum_{k=1}^{3m+c}\frac{k}{3}-\sum_{k=1}^{3m+c}\left\{\frac{k}{3}\right\}$$

$$=\frac{1}{3}\cdot\frac{1}{2}(3m+c)(3m+c+1)$$

$$-m\left(\frac{1}{3}+\frac{2}{3}\right)-\Delta$$

$$=\frac{1}{6}\{(3m+c)^2+(3m+c)\}-m-\Delta$$

$$=\frac{1}{6}\{9m^2+6mc-3m+c^2+c-6\Delta\}.$$

这里

$$\Delta=\begin{cases}0, & c=0,\\ \frac{1}{3}, & c=1,\\ 1, & c=2.\end{cases}$$

由此得

$$c^2 + c = 6\Delta.$$

所以

$$\sum_{k=1}^{n}\left[\frac{k}{3}\right] = \frac{m}{2}(3m + 2c - 1).$$

而

$$\left[\frac{n(n-1)}{6}\right] = \left[\frac{(3m+c)(3m+c-1)}{6}\right]$$

$$= \left[\frac{(3m+c)^2 - (3m+c)}{6}\right]$$

$$= \left[\frac{9m^2 + 6mc - 3m + c^2 - c}{6}\right]$$

$$= \left[\frac{m}{2}(3m + 2c - 1) + \frac{c^2 - c}{6}\right].$$

由于m与 $3m+2c-1$ 必为一奇、一偶，故 $\frac{m}{2}(3m+2c-1)$ 是整数。而 $\frac{c^2-c}{6} < 1$，所以

$$\left[\frac{n(n-1)}{6}\right] = \frac{m}{2}(3m + 2c - 1).$$

(iii) 证：设 $n = am + c$，$0 \leqslant c < a$，则

$$\sum_{k=1}^{n}\left[\frac{k}{a}\right] = \sum_{k=1}^{am+c}\frac{k}{a} - \sum_{k=1}^{am+c}\left\{\frac{k}{a}\right\}$$

$$= \sum_{k=1}^{am+c}\frac{k}{a} - m\sum_{k=1}^{a-1}\frac{k}{a} - \sum_{k=1}^{c}\frac{k}{a}$$

$$= \frac{1}{2a}(am+c)(am+c+1) - \frac{1}{2a}m(a-1)a$$

$$- \frac{1}{2a}c(c+1)$$

$$= \frac{1}{2a}\{(am+c)^2+(am+c)-ma(a-1)$$
$$-c(c+1)\}$$
$$= \frac{1}{2a}\{(am+c)^2+2am-ma^2-c^2\}$$
$$= \frac{1}{2a}\{(am+c)^2+am(2-a)-c^2\}$$
$$= \frac{1}{8a}\{(2am+2c)^2+4am(2-a)-4c^2\}$$
$$= \frac{1}{8a}\{[(2am+2c)+(2-a)]^2$$
$$-4c(2-a)-(2-a)^2-4c^2\}$$
$$= \frac{1}{8a}\{(2n+2-a)^2-(2c+2-a)^2\}.$$

由于

$$(2c+2-a)^2 \leqslant \{2(a-1)+2-a\}^2$$
$$= a^2 < 8a,$$

因此

$$\frac{(2c+2-a)^2}{8a} < 1.$$

而

$$\sum_{k=1}^{n}\left[\frac{k}{a}\right]$$

是整数，故

$$\sum_{k=1}^{n}\left[\frac{k}{a}\right] = \left[\frac{(2n+2-a)^2}{8a}\right].$$

取 $b=2-a$ 就得到了证明。

8. 证：设 $k^2 \leqslant n < (k+1)^2$，及 $n = k^2 + l$，则 $0 \leqslant l < (k+1)^2 - k^2 = 2k+1$，所以

$$\sqrt{4n+2}=\sqrt{4k^2+4l+2}$$
$$\leqslant\sqrt{4k^2+8k+2}<2(k+1)。$$

显然 $\sqrt{4n+2}>2k$，因此

$$2k\leqslant[\sqrt{4n+2}]\leqslant 2k+1.$$

若 $\sqrt{4n+2}\geqslant 2k+1$，则

$$\sqrt{4k^2+4l+2}\geqslant\sqrt{4k^2+4k+1}.$$

即

$$4l+2\geqslant 4k+1,\quad 4l\geqslant 4k-1.$$

由于 l 是整数,因此 $l\geqslant k$.

所以

$$[\sqrt{4n+2}]=\begin{cases}2k+1, & l\geqslant k,\\ 2k, & l<k.\end{cases}$$

而 $l<k$ 时，

$$[\sqrt{n}+\sqrt{n+1}]\leqslant[\sqrt{k^2+k-1}+\sqrt{k^2+k}]$$
$$<\left[2\sqrt{k^2+k+\frac{1}{4}}\right]=2k+1.$$

显然

$$[\sqrt{n}+\sqrt{n+1}]\geqslant 2k,$$

所以 $l<k$ 时，

$$[\sqrt{n}+\sqrt{n+1}]=2k.$$

若 $l\geqslant k$，则

$$[\sqrt{n}+\sqrt{n+1}]\geqslant[\sqrt{k^2+k}+\sqrt{k^2+k+1}]$$
$$\geqslant 2k+1.$$

末一步是由于

$$(\sqrt{k^2+k}+\sqrt{k^2+k+1})^2$$

$$= 2k^2 + 2k + 1 + 2\sqrt{(k^2+k)(k^2+k+1)}$$
$$> 2k^2 + 2k + 1 + 2(k^2+k)$$
$$= (2k+1)^2.$$

又由 $n < (k+1)^2$ 可知

$$[\sqrt{n} + \sqrt{n+1}] \leqslant 2k+1,$$

所以

$$[\sqrt{n} + \sqrt{n+1}] = 2k+1, \quad l \geqslant k.$$

由以上结果就证明了

$$[\sqrt{n} + \sqrt{n+1}] = [\sqrt{4n+2}].$$

9. 证:

$$\sum_{k=0}^{n-1} f\left(x+\frac{k}{n}\right) = \sum_{k=0}^{n-1}\left\{\left(x+\frac{k}{n}-\frac{1}{2}\right)-\left[x+\frac{k}{n}\right]\right\}$$
$$= n\left(x-\frac{1}{2}\right)+\frac{1}{n}\cdot\frac{1}{2}n(n-1)-\sum_{k=0}^{n-1}\left[x+\frac{k}{n}\right]$$
$$= nx-\frac{1}{2}-\sum_{k=0}^{n-1}\left[x+\frac{k}{n}\right].$$

由例 22 得

$$\sum_{k=0}^{n-1}\left[x+\frac{k}{n}\right] = [nx].$$

所以

$$\sum_{k=0}^{n-1} f\left(x+\frac{k}{n}\right) = nx - [nx] - \frac{1}{2} = f(nx).$$

10. 证: 设 $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_m^{\alpha_m}$.

由引理 6 知

$$d(n) = (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_m+1).$$

若 $d(n)$ 是奇数,则必须所有 α_i ($1 \leqslant i \leqslant m$) 为偶数.

设

$$\alpha_i = 2\beta_i, \quad 1 \leqslant i \leqslant m,$$

则

$$n = (p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m})^2.$$

所以 n 是平方数。

反之若 n 是平方数，设 $n = n_0^2$，n_0 是整数，则

$$n_0 = p_1^{\alpha_1/2} p_2^{\alpha_2/2} \cdots p_m^{\alpha_m/2}.$$

所以 $2 | \alpha_i$，$1 \leqslant i \leqslant m$。即所有的 $\alpha_i + 1$ 是奇数，因此 $d(n)$ 是奇数。

11. 证：设 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. 若 $m = 1$，则 $n = p_1^{\alpha_1}$. 它的所有因数是 $1, p_1, \cdots, p_1^{\alpha_1}$，因此

$$\prod_{t|n} t = \prod_{j=0}^{\alpha_1} p_1^j = p_1^{\frac{1}{2}\alpha_1(\alpha_1+1)} = (p_1^{\alpha_1})^{\frac{1}{2}(\alpha_1+1)} = n^{d(n)/2}.$$

所以 $m = 1$ 时命题成立. 现假设命题在 $m = k - 1$ 时成立，即假设 $n_1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k-1}^{\alpha_{k-1}}$ 时有

$$\prod_{t|n_1} t = n_1^{d(n_1)/2},$$

则当 $m = k$ 时，$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = n_1 p_k^{\alpha_k}$，它的因数是 n_1 的因数和 $p_k^{\alpha_k}$ 的因数的乘积. 所以由归纳法的假定得

$$\begin{aligned}\prod_{t|n} t &= \prod_{t_1|n_1} \prod_{t_2|p_k^{\alpha_k}} t_1 t_2 = \prod_{t_1|n_1} t_1^{d(p_k^{\alpha_k})} \cdot (p_k^{\alpha_k})^{d(p_k^{\alpha_k})/2} \\ &= \{n_1^{d(n_1)/2}\}^{d(p_k^{\alpha_k})} \cdot \{p_k^{\alpha_k}\}^{d(n_1)d(p_k^{\alpha_k})/2} \\ &= \{n_1 p_k^{\alpha_k}\}^{d(n_1)d(p_k^{\alpha_k})/2}.\end{aligned}$$

因 $(n_1, p_k^{\alpha_k}) = 1$，由引理 7 得 $d(n) = d(n_1)d(p_k^{\alpha_k})$，所以

$$\prod_{t|n} t = n^{d(n)/2}.$$

12. 证：由 $\mu(n)$ 的定义可得

$$\mu^2(n)=\begin{cases}1, & n \text{ 不含平方因子},\\ 0, & n \text{ 含有平方因子}.\end{cases}$$

当 n 不含平方因子时 $\sum\limits_{d^2\mid n}\mu(d)=\mu(1)=1$． n 含有平方因子时，设 $n=n_0^2m$， $n_0>1$，m 不含平方因子，则

$$\sum_{d^2\mid n}\mu(d)=\sum_{d\mid n_0}\mu(d)=0.$$

13. 证：由假设条件

$$\sum_{d\mid n}F\left(\frac{n}{d}\right)\mu(d)=\sum_{d\mid n}\mu(d)\sum_{c\mid \frac{n}{d}}f(c)$$

$$=\sum_{cd\mid n}\mu(d)f(c)=\sum_{c\mid n}f(c)\sum_{d\mid \frac{n}{c}}\mu(d).$$

而

$$\sum_{d\mid \frac{n}{c}}\mu(d)=\begin{cases}1, & \text{当 } c=n,\\ 0, & \text{其它情形},\end{cases}$$

所以

$$\sum_{d\mid n}F\left(\frac{n}{d}\right)\mu(d)=f(n).$$

用类似的方法可证明其逆亦成立.

14. 设 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$.

(i) 证:

$$\sum_{d\mid p_s^{\alpha_s}}\varphi(d)=\varphi(1)+\varphi(p_s)+\varphi(p_s^2)+\cdots+\varphi(p_s^{\alpha_s})$$

$$=1+(p_s-1)+(p_s^2-p_s)+\cdots$$
$$+(p_s^{\alpha_s}-p_s^{\alpha_s-1})=p_s^{\alpha_s},$$

所以

$$\sum_{d|n}\varphi(d)=\sum_{d_1|p_1^{\alpha_1}}\cdots\sum_{d_k|p_k^{\alpha_k}}\varphi(d_1\cdots d_k)$$

$$=\sum_{d_1|p_1^{\alpha_1}}\varphi(d_1)\sum_{d_2|p_2^{\alpha_2}}\varphi(d_2)\cdots\sum_{d_k|p_k^{\alpha_k}}\varphi(d_k)$$

$$=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}=n.$$

(ii) 证：上题中取 $f(d)=\varphi(d)$，$F(n)=n$，则由上题的结论和本题的 (i) 就得到了证明.

15. 证：设N是偶完全数，可写成 $N=2^{n-1}b$，$n>1$，b 是奇数. 由引理 11 和引理 9 得

$$\sigma(N)=\sigma(2^{n-1})\sigma(b)=(2^n-1)\sigma(b).$$

由于N是完全数，故

$$\sigma(N)=2N=2^nb.$$

所以

$$2^nb=(2^n-1)\sigma(b).$$

即

$$\frac{b}{\sigma(b)}=\frac{2^n-1}{2^n}.$$

等式右边是既约分数，因此有

$$b=(2^n-1)c,\quad \sigma(b)=2^nc,\quad c\text{ 是整数}.$$

若 $c>1$，则 b 的因数包含 1，b，2^n-1，c，所以

$$\sigma(b)\geqslant 1+b+2^n-1+c=(2^n-1)c+2^n+c$$
$$=2^n(c+1).$$

但

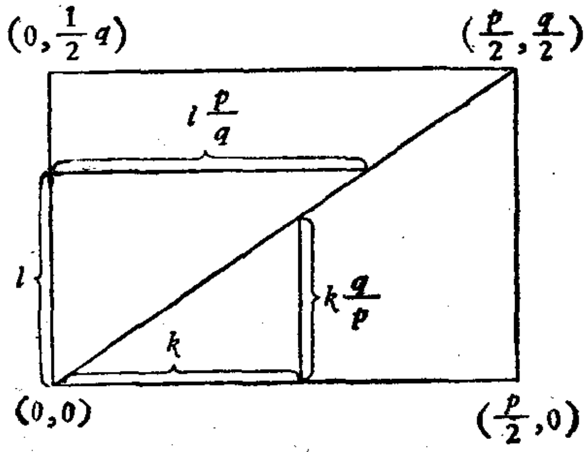
$$\sigma(b)=2^nc<2^n(c+1),$$

因而产生矛盾. 于是 $c=1$，所以 $b=2^n-1$，

$$N=2^{n-1}(2^n-1),\quad \sigma(b)=2^n.$$

即 $\sigma(2^n-1)=2^n$. 假若 2^n-1 不是素数，则 2^n-1 的因数除了 2^n-1 和 1 外，还有别的因数存在，则必有 $\sigma(2^n-1)>2^n$，这与 $\sigma(2^n-1)=2^n$ 矛盾，所以 2^n-1 是素数.

16. 证明：以 $(0,0)$，$\left(0, \frac{1}{2}q\right)$，$\left(\frac{1}{2}p, 0\right)$，$\left(\frac{1}{2}p, \frac{1}{2}q\right)$ 为顶点作长方形.



假若对角线上有整点（二坐标都是整数），则由比例关系得到 $k\frac{q}{p}$ 为整数，即 $p|k$. 这时点在长方形之外了，所以长方形内的对角线上无整点. 因为 p q 是奇数，不大于 $\frac{p}{2}$，$\frac{q}{2}$ 的最大整数分别是 $\frac{p-1}{2}$，$\frac{q-1}{2}$，所以长方形内的整点总数是 $\frac{p-1}{2}\cdot\frac{q-1}{2}$.

对角线下的三角形内的整点数显然是

$$\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right]=\sum_{0<k<\frac{p}{2}}\left[\frac{q}{p}k\right].$$

对角线上的三角形内的整点数是

$$\sum_{l=1}^{\frac{1}{2}(q-1)}\left[l\frac{p}{q}\right]=\sum_{0<l<\frac{q}{2}}\left[\frac{p}{q}l\right].$$

所以

$$\sum_{0<l<\frac{q}{2}}\left[\frac{p}{q}l\right]+\sum_{0<k<\frac{p}{2}}\left[\frac{q}{p}k\right]=\frac{p-1}{2}\cdot\frac{q-1}{2}.$$

第八章

1.（i）解：

$$-4x+8yi+7=2x-3yi+7i.$$

移项

$$-6x+11yi=-7+7i,$$

所以

$$x=\frac{7}{6},\quad y=\frac{7}{11}.$$

(ii) 解:

$$x+yi=\sqrt{a+bi}$$

两边平方得

$$x^2-y^2+2xyi=a+bi,$$

所以

$$\begin{cases}x^2-y^2=a, & (1)\\ 2xy=b. & (2)\end{cases}$$

将两式分别平方后再相加得

$$(x^2-y^2)^2+4x^2y^2=a^2+b^2,$$

即
$$(x^2+y^2)^2=a^2+b^2,$$

$$x^2+y^2=\sqrt{a^2+b^2}. \tag{3}$$

由(1),(3)两式解出

$$x^2=\frac{\sqrt{a^2+b^2}+a}{2},\quad y^2=\frac{\sqrt{a^2+b^2}-a}{2},$$

所以

$$x=\pm\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}},\quad y=\pm\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}.$$

由(2)式可知, $b>0$ 时 x, y 取同号,而 $b<0$ 时, x, y 取异号.

2. 证: 设 $z_1=a+bi$, $z_2=c+di$, 则

$$\begin{aligned}&|z_1-z_2|^2-(|z_1|-|z_2|)^2\\ &=(a-c)^2+(b-d)^2-(\sqrt{a^2+b^2}-\sqrt{c^2+d^2})^2\\ &=2(-ac-bd+\sqrt{a^2+b^2}\cdot\sqrt{c^2+d^2}).\end{aligned}$$

由于

$$(a^2+b^2)(c^2+d^2)-(ac+bd)^2$$
$$=(bc-ad)^2\geqslant 0$$

所以

$$\sqrt{a^2+b^2}\cdot\sqrt{c^2+d^2}\geqslant |ac+bd|.$$

因此得到

$$|z_1-z_2|^2-(|z_1|-|z_2|)^2\geqslant 0,$$
$$|z_1-z_2|>||z_1|-|z_2||.$$

3. 解：设 α 是 27 的立方根，所以

$$\alpha^3=27=27e^{2k\pi i},$$
$$\alpha=3e^{\frac{2k\pi}{3}i}.$$

当 k 取所有整数时只有三个不同的根：

$$\alpha_1=3,\quad \alpha_2=3e^{\frac{2\pi}{3}i}=3(\cos 120^\circ+i\sin 120^\circ),$$
$$\alpha_3=3e^{\frac{4\pi}{3}i}=3(\cos 240^\circ+i\sin 240^\circ).$$

4. (i) 证：由引理 2 和 (24) 式得

$$e^{3\alpha i}=(e^{\alpha i})^3=(\cos\alpha+i\sin\alpha)^3$$
$$=\cos^3\alpha+3\cos^2\alpha(i\sin\alpha)+3\cos\alpha(i\sin\alpha)^2+(i\sin\alpha)^3$$
$$=(\cos^3\alpha-3\cos\alpha\sin^2\alpha)+i(3\cos^2\alpha\sin\alpha-\sin^3\alpha).$$

而由定义

$$e^{3\alpha i}=\cos 3\alpha+i\sin 3\alpha.$$

分别由实部相等和虚部相等得到

$$\sin 3\alpha=3\cos^2\alpha\sin\alpha-\sin^3\alpha$$
$$=3(1-\sin^2\alpha)\sin\alpha-\sin^3\alpha$$
$$=3\sin\alpha-4\sin^3\alpha,$$
$$\cos 3\alpha=\cos^3\alpha-3\cos\alpha\sin^2\alpha$$
$$=\cos^3\alpha-3\cos\alpha(1-\cos^2\alpha)$$
$$=4\cos^3\alpha-3\cos\alpha.$$

(ii) 证：由引理 2

$$
\begin{aligned}
e^{4\alpha i} &= (e^{\alpha i})^4 = [(\cos\alpha + i\sin\alpha)^2]^2 \\
&= (\cos^2\alpha - \sin^2\alpha + 2i\sin\alpha\cos\alpha)^2 \\
&= (\cos^2\alpha - \sin^2\alpha)^2 - 4\sin^2\alpha\cos^2\alpha \\
&\quad + 4i\sin\alpha\cos\alpha(\cos^2\alpha - \sin^2\alpha) \\
&= \cos^4\alpha - 6\sin^2\alpha\cos^2\alpha + \sin^4\alpha \\
&\quad + i(4\sin\alpha\cos^3\alpha - 4\sin^3\alpha\cos\alpha).
\end{aligned}
$$

而

$$
e^{4\alpha i} = \cos 4\alpha + i\sin 4\alpha.
$$

上两式的实部和虚部分别相等就得到了证明.

(iii) 证：由定义

$$
\begin{aligned}
e^{i\alpha} &= \cos\alpha + i\sin\alpha, \\
e^{-i\alpha} &= \cos(-\alpha) + i\sin(-\alpha) \\
&= \cos\alpha - i\sin\alpha,
\end{aligned}
$$

所以

$$
\cos\alpha = \frac{e^{i\alpha} + e^{-i\alpha}}{2},
$$

$$
\begin{aligned}
\cos^4\alpha &= \left(\frac{e^{i\alpha} + e^{-i\alpha}}{2}\right)^4 \\
&= \frac{1}{16}[(e^{i\alpha} + e^{-i\alpha})^2]^2 \\
&= \frac{1}{16}[e^{2i\alpha} + e^{-2i\alpha} + 2]^2 \\
&= \frac{1}{16}[(e^{2i\alpha} + e^{-2i\alpha})^2 + 4(e^{2i\alpha} + e^{-2i\alpha}) + 4] \\
&= \frac{1}{8}\left[\frac{e^{4i\alpha} + e^{-4i\alpha}}{2} + 4\frac{e^{2i\alpha} + e^{-2i\alpha}}{2} + 3\right] \\
&= \frac{1}{8}(\cos 4\alpha + 4\cos 2\alpha + 3).
\end{aligned}
$$

(iv) 证：由 (iii) 类似地可得到

$$\sin\alpha = \frac{e^{i\alpha} - e^{-i\alpha}}{2i},$$

所以

$$\begin{aligned}\sin^3\alpha &= \left(\frac{e^{i\alpha} - e^{-i\alpha}}{2i}\right)^3\\ &= \frac{e^{3i\alpha} - 3(e^{i\alpha})^2(e^{-i\alpha}) + 3e^{i\alpha}(e^{-i\alpha})^2 - (e^{-i\alpha})^3}{(2i)^3}\\ &= -\frac{1}{4}\left(\frac{e^{3i\alpha} - e^{-3i\alpha}}{2i} - 3\,\frac{e^{i\alpha} - e^{-i\alpha}}{2i}\right)\\ &= -\frac{1}{4}(\sin 3\alpha - 3\sin\alpha).\end{aligned}$$

5. (i) 证：由 (19) 式中取 $\beta = \alpha$ 以及由 (20) 式得

$$\cos 2\alpha = \cos^2\alpha - \sin^2\alpha = 1 - 2\sin^2\alpha,$$

所以

$$\sin^2\alpha = \frac{1 - \cos 2\alpha}{2}.$$

同样

$$\sin^2 2\alpha = \frac{1 - \cos 4\alpha}{2},$$

$$\sin^2 3\alpha = \frac{1 - \cos 6\alpha}{2}.$$

各式相加得

$$\sum_{k=1}^{n}\sin^2 k\alpha = \sum_{k=1}^{n}\frac{1 - \cos 2k\alpha}{2} = \frac{n}{2} - \frac{1}{2}\sum_{k=1}^{n}\cos 2k\alpha.$$

在 (39) 式中取 $\theta = 2\alpha$ 得

$$\sum_{k=1}^{n}\cos 2k\alpha = \frac{\sin n\alpha}{\sin\alpha}\cos(n+1)\alpha,$$

所以

$$\sum_{k=1}^{n}\sin^2 k\alpha=\frac{1}{2}\left\{n-\frac{\sin n\alpha}{\sin\alpha}\cos(n+1)\alpha\right\}$$

$$=\frac{1}{2}\left\{n-\frac{1}{\sin\alpha}[\sin(2n+1)\alpha-\cos n\alpha\sin(n+1)\alpha]\right\}$$

$$=\frac{1}{2}\left\{n-\frac{1}{\sin\alpha}[\sin(2n+1)\alpha\right.$$

$$\left.-\cos n\alpha(\sin n\alpha\cos\alpha+\sin\alpha\cos n\alpha)]\right\}$$

$$=\frac{1}{2}\left\{n-\frac{1}{\sin\alpha}\left[\sin(2n+1)\alpha-\frac{1}{2}\sin 2n\alpha\cos\alpha\right.\right.$$

$$\left.\left.-\sin\alpha\frac{\cos 2n\alpha+1}{2}\right]\right\}$$

$$=\frac{1}{2}\left\{n-\frac{1}{\sin\alpha}\left[\frac{1}{2}\sin(2n+1)\alpha-\frac{1}{2}\sin\alpha\right]\right\}$$

$$=\frac{1}{4\sin\alpha}[(2n+1)\sin\alpha-\sin(2n+1)\alpha].$$

(ii) 证：由第 4 题(i) 得

$$\cos^3\alpha=\frac{1}{4}(3\cos\alpha+\cos 3\alpha).$$

将 α 换成 $k\alpha$ 就得到

$$\cos^3 k\alpha=\frac{1}{4}(3\cos k\alpha+\cos 3k\alpha).$$

对 $k=1,2,\cdots,n$ 求和得

$$\sum_{k=1}^{n}\cos^3 k\alpha=\frac{1}{4}\left[3\sum_{k=1}^{n}\cos k\alpha+\sum_{k=1}^{n}\cos 3k\alpha\right].$$

由 (39) 式得到

$$\sum_{k=1}^{n}\cos k\alpha=\frac{\sin\frac{n\alpha}{2}}{\sin\frac{\alpha}{2}}\cos\frac{(n+1)\alpha}{2}.$$

将 α 换以 3α 得

$$\sum_{k=1}^{n}\cos 3k\alpha=\frac{\sin\frac{3n\alpha}{2}}{\sin\frac{3\alpha}{2}}\cos\frac{3(n+1)\alpha}{2}.$$

所以

$$\sum_{k=1}^{n}\cos^{3}k\alpha=\frac{1}{4}\left[\frac{3\sin\frac{n\alpha}{2}}{\sin\frac{\alpha}{2}}\cos\frac{(n+1)\alpha}{2}\right.$$

$$\left.+\frac{\sin\frac{3n\alpha}{2}}{\sin\frac{3\alpha}{2}}\cos\frac{3(n+1)\alpha}{2}\right].$$

6. 证:

$$\begin{aligned}
&\frac{1+\sin\theta+i\cos\theta}{1+\sin\theta-i\cos\theta}\\
&\quad=\frac{(1+\sin\theta+i\cos\theta)^{2}}{(1+\sin\theta)^{2}+\cos^{2}\theta}\\
&\quad=\frac{(1+\sin\theta)^{2}-\cos^{2}\theta+2i(1+\sin\theta)\cos\theta}{1+2\sin\theta+\sin^{2}\theta+\cos^{2}\theta}\\
&\quad=\frac{1+2\sin\theta+\sin^{2}\theta-(1-\sin^{2}\theta)+2i(1+\sin\theta)\cos\theta}{2(1+\sin\theta)}\\
&\quad=\frac{2\sin\theta(1+\sin\theta)+i2(1+\sin\theta)\cos\theta}{2(1+\sin\theta)}\\
&\quad=\sin\theta+i\cos\theta.
\end{aligned}$$

在上式中取 $\theta=\frac{\pi}{5}$, 得

$$\frac{1+\sin\frac{\pi}{5}+i\cos\frac{\pi}{5}}{1+\sin\frac{\pi}{5}-i\cos\frac{\pi}{5}}=\sin\frac{\pi}{5}+i\cos\frac{\pi}{5}.$$

两边取五次方，并由本章例 8 得

$$\frac{\left(1+\sin\frac{\pi}{5}+i\cos\frac{\pi}{5}\right)^5}{\left(1+\sin\frac{\pi}{5}-i\cos\frac{\pi}{5}\right)^5}=\left(\sin\frac{\pi}{5}+i\cos\frac{\pi}{5}\right)^5$$

$$=e^{i5\left(\frac{\pi}{2}-\frac{\pi}{5}\right)}=e^{i\frac{3}{2}\pi}$$

$$=\cos\frac{3}{2}\pi+i\sin\frac{3}{2}\pi=-i,$$

所以

$$\left(1+\sin\frac{\pi}{5}+i\cos\frac{\pi}{5}\right)^5+i\left(1+\sin\frac{\pi}{5}-i\cos\frac{\pi}{5}\right)^5=0.$$

7. 解：作复数 A_n+iB_n.

$$\begin{aligned}A_n+iB_n&=1+r(\cos\theta+i\sin\theta)+r^2(\cos 2\theta\\&\quad+i\sin 2\theta)+\cdots\\&\quad+r^{n-1}[\cos(n-1)\theta+i\sin(n-1)\theta]\\&=1+re^{i\theta}+r^2e^{i2\theta}+\cdots+r^{n-1}e^{i(n-1)\theta}.\end{aligned}$$

令 $z=re^{i\theta}$，并由引理 3 得

$$A_n+iB_n=1+z+z^2+\cdots+z^{n-1}=\frac{1-z^n}{1-z}$$

$$=\frac{1-r^ne^{in\theta}}{1-re^{i\theta}}=\frac{(1-r^ne^{in\theta})(1-re^{-i\theta})}{(1-re^{i\theta})(1-re^{-i\theta})}$$

$$=\frac{1-re^{-i\theta}-r^ne^{in\theta}+r^{n+1}e^{i(n-1)\theta}}{1-r(e^{i\theta}+e^{-i\theta})+r^2}$$

$$=\frac{1-r\cos\theta-r^n\cos n\theta+r^{n+1}\cos(n-1)\theta}{1-2r\cos\theta+r^2}$$

$$+\frac{r\sin\theta-r^n\sin n\theta+r^{n+1}\sin(n-1)\theta}{1-2r\cos\theta+r^2}i.$$

比较实数部分和虚数部分可得

$$A_n = \frac{1 - r\cos\theta - r^n\cos n\theta + r^{n+1}\cos(n-1)\theta}{1 - 2r\cos\theta + r^2},$$

$$B_n = \frac{r\sin\theta - r^n\sin n\theta + r^{n+1}\sin(n-1)\theta}{1 - 2r\cos\theta + r^2}.$$

8. 证：在上一题中取 $r = \cos\theta$，由于 $\theta \neq m\pi$，所以 $|r| < 1$，当 $n \to \infty$ 时，$r^n \to 0$，$r^{n+1} \to 0$，因此 $r^n\cos n\theta \to 0$，$r^{n+1}\cos(n-1)\theta \to 0$。由上题的结果，当 $n \to \infty$ 时

$$A_n = \frac{1 - \cos^2\theta}{1 - 2\cos^2\theta + \cos^2\theta} = 1.$$

而由 A_n 的定义，当 $n \to \infty$ 时

$$A_n = 1 + \sum_{k=1}^{\infty} r^k \cos k\theta = 1 + \sum_{k=1}^{\infty} \cos^k\theta\cos k\theta,$$

所以

$$\sum_{k=1}^{\infty} \cos^k\theta\cos k\theta = 0.$$

若 $\cos\theta \neq 0$，则上式两边同除以 $\cos\theta$，得到

$$\sum_{k=1}^{\infty} \cos^{k-1}\theta\cos k\theta = 0.$$

若 $\cos\theta = 0$，则由于

$$\sum_{k=1}^{\infty} \cos^{k-1}\theta\cos k\theta$$

中每项都有因子 $\cos\theta$，所以每项都是 0。结果显然成立。

9. 证：

$$\text{左边} = \sum_{k=1}^{n} [\cos(4k-3)\alpha + \sin(4k-1)\alpha]$$

$$= \sum_{k=0}^{n-1} \cos(4k+1)\alpha + \sum_{k=0}^{n-1} \sin(4k+3)\alpha.$$

在 (37) 式中令 $\theta = \alpha$，$\varphi = 4\alpha$，得

$$\sum_{k=0}^{n-1}\cos(4k+1)\alpha=\frac{\sin 2n\alpha}{\sin 2\alpha}\cos(2n-1)\alpha.$$

在(38)式中令 $\theta=3\alpha$，$\varphi=4\alpha$，得

$$\sum_{k=0}^{n-1}\sin(4k+3)\alpha=\frac{\sin 2n\alpha}{\sin 2\alpha}\sin(2n+1)\alpha.$$

而上两式成立的条件 $\left\{\frac{\varphi}{2\pi}\right\}\neq 0$ 相当于 $\alpha\neq\frac{k}{2}\pi$，

所以

$$\begin{aligned}
&\cos\alpha+\sin 3\alpha+\cos 5\alpha+\sin 7\alpha+\cdots+\sin(4n-1)\alpha\\
&=\frac{\sin 2n\alpha}{\sin 2\alpha}[\cos(2n-1)\alpha+\sin(2n+1)\alpha]\\
&=\frac{\sin 2n\alpha}{\sin 2\alpha}[\cos 2n\alpha\cos\alpha+\sin 2n\alpha\sin\alpha\\
&\quad+\sin 2n\alpha\cos\alpha+\cos 2n\alpha\sin\alpha]\\
&=\frac{\sin 2n\alpha}{\sin 2\alpha}(\cos 2n\alpha+\sin 2n\alpha)(\cos\alpha+\sin\alpha).
\end{aligned}$$

10. 证：$\left\{\frac{\theta}{\pi}\right\}=0$ 时显然成立. $\left\{\frac{\theta}{\pi}\right\}\neq 0$ 时由(41),(42)得

$$\sin\alpha+\sin 3\alpha+\cdots+\sin(2n-1)\alpha=\frac{\sin n\alpha}{\sin\alpha}\sin n\alpha,$$

$$\cos\alpha+\cos 3\alpha+\cdots+\cos(2n-1)\alpha=\frac{\sin n\alpha}{\sin\alpha}\cos n\alpha.$$

两式相除就得到

$$\operatorname{tg} n\alpha=\frac{\sin\alpha+\sin 3\alpha+\cdots+\sin(2n-1)\alpha}{\cos\alpha+\cos 3\alpha+\cdots+\cos(2n-1)\alpha}.$$

11. 证明：设 $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$，$m_s=p_s^{\alpha_s}$，$1\leqslant s\leqslant n$，定义 $M_s=\frac{m}{m_s}$. 又设 $\xi_1,\xi_2,\cdots,\xi_n$ 分别通过与模 $m_1,m_2,\cdots,m_n$ 互

素的剩余系.由第五章的习题可知 $\xi_1 M_1+\xi_2 M_2+\cdots+\xi_n M_k$ 通过与模 m 互素的剩余系,所以

$$\sum_{\xi_1,\cdots,\xi_n}\left\{\frac{\xi_1}{m_1}+\frac{\xi_2}{m_2}+\cdots+\frac{\xi_n}{m_n}\right\}$$

$$=\sum_{\xi_1,\cdots,\xi_n}\left\{\frac{\xi_1 M_1+\xi_2 M_2+\cdots+\xi_k M_k}{m}\right\}=\sum_{\xi}\left\{\frac{\xi}{m}\right\}.$$

$$\sum_{\xi} e^{2\pi i\frac{\xi}{m}}=\sum_{\xi} e^{2\pi i\left\{\frac{\xi}{m}\right\}+2\pi i\left[\frac{\xi}{m}\right]}=\sum_{\xi} e^{2\pi i\left\{\frac{\xi}{m}\right\}}$$

$$=\sum_{\xi_1} e^{2\pi i\left\{\frac{\xi_1}{m_1}\right\}}\sum_{\xi_2} e^{2\pi i\left\{\frac{\xi_2}{m_2}\right\}}\cdots\sum_{\xi_n} e^{2\pi i\left\{\frac{\xi_n}{m_n}\right\}}.$$

若 m 不含有平方因子,则 $\alpha_s=1,\ 1\leqslant s\leqslant n$.

$$\sum_{\xi_s} e^{2\pi i\left\{\frac{\xi_s}{m_s}\right\}}=\sum_{\xi_s=1}^{p_s-1} e^{2\pi i\frac{\xi_s}{p_s}}=\sum_{\xi_s=1}^{p_s} e^{2\pi i\frac{\xi_s}{p_s}}-1=-1,$$

所以

$$\sum_{\xi} e^{2\pi i\frac{\xi}{m}}=(-1)^n.$$

若 m 含有平方因子,则至少有一个 $\alpha_s>1$, 这时令 $m_s=p_s m_s'$, 在 $1,2,\cdots,p_s^{\alpha_s}$ 中只有 kp_s, $k=1,2,\cdots,p_s^{\alpha_s-1}$ 与 $p_s^{\alpha_s}$ 不互素,所以由引理 5

$$\sum_{\xi_s} e^{2\pi i\left\{\frac{\xi_s}{m_s}\right\}}=\sum_{\xi_s=1}^{p_s^{\alpha_s}} e^{2\pi i\frac{\xi_s}{p_s^{\alpha_s}}}-\sum_{k=1}^{p_s^{\alpha_s-1}} e^{2\pi i\frac{kp_s}{p_s^{\alpha_s}}}$$

$$=\sum_{\xi_s=1}^{p_s^{\alpha_s}} e^{2\pi i\frac{\xi_s}{p_s^{\alpha_s}}}-\sum_{k=1}^{p_s^{\alpha_s-1}} e^{2\pi i\frac{k}{p_s^{\alpha_s-1}}}=0.$$

因此由 $\mu(m)$ 的定义得到

$$\mu(m)=\sum_{\xi} e^{2\pi i\frac{\xi}{m}}.$$

12. 证: 由于 $(2A,m)=1$, 由第四章引理 12 知同余式 $2Ax'\equiv a\pmod m$ 有解 x',所以

$$\left|\sum_{x=0}^{m-1} e^{2\pi i \frac{Ax^2+ax}{m}}\right| = \left|\sum_{x=0}^{m-1} e^{2\pi i \frac{Ax^2+2Ax'x}{m}}\right|$$

$$= \left|\sum_{x=0}^{m-1} e^{2\pi i \frac{Ax^2+2Ax'x}{m}}\right| \cdot \left|e^{2\pi i \frac{Ax'^2}{m}}\right|$$

$$= \left|\sum_{x=0}^{m-1} e^{2\pi i \frac{A(x+x')^2}{m}}\right| = \left|\sum_{x=x'}^{m+x'-1} e^{2\pi i \frac{Ax^2}{m}}\right|$$

$$= \left|\sum_{x=x'}^{m-1} e^{2\pi i \frac{Ax}{m}} + \sum_{x=m}^{m+x'-1} e^{2\pi i \frac{Ax^2}{m}}\right|$$

$$= \left|\sum_{x=x'}^{m-1} e^{2\pi i \frac{Ax^2}{m}} + \sum_{x=0}^{x'-1} e^{2\pi i \frac{Ax^2}{m}}\right|$$

$$= \left|\sum_{x=0}^{m-1} e^{2\pi i \frac{Ax^2}{m}}\right| \quad = S(A, m).$$

由 $(2A, m) = 1$ 可知m是奇数，因而由引理 9 可知

$$S(A, m) = \sqrt{m}.$$

13. 证:

$$S(nm', m)S(nm, m') = \left(\sum_{x=0}^{m-1} e^{2\pi i \frac{nm'x^2}{m}}\right)\left(\sum_{x'=0}^{m'-1} e^{2\pi i \frac{nmx'^2}{m'}}\right)$$

$$= \sum_{x=0}^{m-1}\sum_{x'=0}^{m'-1} e^{2\pi i \left(\frac{nm'x^2}{m} + \frac{nmx'^2}{m'}\right)}$$

$$= \sum_{x=0}^{m-1}\sum_{x'=0}^{m'-1} e^{2\pi i \frac{n(m'^2x^2+m^2x'^2)}{mm'}}.$$

由第五章习题 1 可知当 x, x' 分别通过模 m, m' 的完全剩余系时，$N = m'x + mx'$ 就通过模 mm' 的完全剩余系，且

$$nN^2 = n(m'x + mx')^2 \equiv n(m'^2x^2 + m^2x'^2) \pmod{mm'},$$

因此

$$S(nm', m)S(nm, m') = \sum_{N=0}^{mm'-1} e^{2\pi i \frac{nN^2}{mm'}}$$

$$= S(n, mm').$$

14. (i) 证:

$$C_q(m)C_{q'}(m) = \sum_h e^{2\pi i \frac{hm}{q}} \cdot \sum_{h'} e^{2\pi i \frac{h'm}{q'}}$$

$$= \sum_h \sum_{h'} e^{2\pi i m\left(\frac{h}{q}+\frac{h'}{q'}\right)}$$

$$= \sum_h \sum_{h'} e^{2\pi i m \frac{hq'+h'q}{qq'}}.$$

由第五章习题 7 可知当 h, h' 分别通过与模 q, q' 互素的剩余系时, $N = hq' + h'q$ 通过与模 qq' 互素的剩余系,所以

$$C_q(m)C_{q'}(m) = \sum_N e^{2\pi i \frac{mN}{qq'}}$$

$$= C_{qq'}(m).$$

(ii) 证: 由定义

$$\sum_{d|q} C_d(m) = \sum_{d|q} \sum_k e^{2\pi i \frac{km}{d}}$$

$$= \sum_{d|q} \sum_k e^{2\pi i \frac{kd'm}{q}}.$$

这里 $q = dd'$, k 通过与模 d 互素的剩余系. 上式右边的项数总共有 $\sum\limits_{d|q} \varphi(d) = q$ 项(第七章 14 题). 设 $h = kd' = k\frac{q}{d}$. 下面证明这 q 项中的 h 对模 q 两两不同余. 设若

$$h_1 \equiv h_2 \pmod q,$$

即

$$k_1 \frac{q_1}{d_1} \equiv k_2 \frac{q}{d_2} \pmod q,$$

所以

$$k_1 d_2 \equiv k_2 d_1 \pmod{d_1 d_2}.$$

由于

$$(k_1, d_1) = 1, \quad (k_2, d_2) = 1,$$

因而有

$$d_1 = d_2,\quad k_1 = k_2,\quad h_1 = h_2.$$

因此 h 通过模 q 的完全剩余系．所以

$$\sum_{d|q} C_d(m) = \sum_h e^{2\pi i \frac{hm}{q}} = f(q).$$

由引理 18 得到

$$f(q) = \sum_{h=0}^{q-1} e^{2\pi i \frac{mh}{q}} = \begin{cases} q, & \text{当 } q|m; \\ 0, & \text{当 } q\nmid m. \end{cases}$$

由上面二式及第七章 13 题立即得到

$$\begin{aligned} C_q(m) &= \sum_{d|q} \mu(d) f\left(\frac{q}{d}\right) \\ &= \sum_{d|q} \mu\left(\frac{q}{d}\right) f(d) \\ &= \sum_{d|q,\, d|m} \mu\left(\frac{q}{d}\right) d. \end{aligned}$$

当 $m = 1$ 时得到

$$C_q(1) = \mu(q).$$

于是得到了 11 题的又一证明．

勘　误（第Ⅰ册）

页数	行数	误	正
71	8	…硬币共十枚，付给一角八分钱，	…硬币共十枚，币值共一角八分钱，
110	倒16	$2^7\times5-1)(2^7)^4+1=(1+2^7\times5)(2^7)^4+1-(2^7)^4=$	$2^7\times5-5^4)(2^7)^4+1=(1+2^7\times5)(2^7)^4+1-(5\times2^7)^4=$